INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Defense Information Infrastructure Master Plan: Overview

B. DATE Report Downloaded From the Internet: 7 May 98

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #: Assistant Secretary of Defense

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __PM__ **Preparation Date:** 7 May 98

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.

DEFENSE INFORMATION INFRASTRUCTURE MASTER PLAN: OVERVIEW

VERSION 7.0

---

13 March 1998

Acknowledgments

The key element of the DII is people. The people listed here prodaced this document.

Section 'Authors

Mr. Richard Allen
LCDR Ann Bennett
Mr. Irv Boyles
Mr. Jack Bryant
Ms. Alice Campbell
Ms. Carolyn Collier
Mr. Marty Costellic
Mr, Ralph Dantinne
M4j Brian Eleazer
Mr. Dwight T. Ford
LIC Bob Forsyth
Mr. Steve Goya
Ms. Cynthia Gardner
Cot Warren Grant
Mr. Terry Hagle
Mr, Don Hall
Mr. George Hoehl
Mr. Goodwin Hurrol
Mr, Rick Larson
LTC Nick Lebano
LTC Richard Logsdon
Dr. Fred Moxlcy
Ms. Marti Pickens
Mr. Ron Pirshvalko
Mr. Mike Roberson
Ma] Bill Scheppers
Ms. Karen Setz
Mr. Dave Shelly
Lt Cot Skillman
Ms. Joanne Spriggs
Ms. Cher Terry
Mr. Gary. Thurston
Mr. John Todd
Ms. Geraldine Versis
Mr. Rob Vietmeyer
Mr. Mario Vizcarra
Mr. Keith Weber
Mr. Jim Whittake

Department and Agency Points of Contact

ARPA---------- Mr. Brian Sosdian
ASD(C3I)---------- Mr..Kevin Meyers
ASD(RA)---------- Ms. Ellen Embry
AETC---------- Ms. Julie Barrow
DDR&E---------- Ms. Lorraine Williams
DFAS---------- Mr. Marty Costellic
DIA\DoDIIS---------- Maj Bernise Beckwith
DISA---------- Mr. Len Tabacchi
DLA---------- Mr. James Livengood
DMIM---------- Ms. Alice Campbell
DMSO---------- Mr. Chris Turrell
DoDIIS---------- Ms. Sue Goodman
DOS---------- CDL John Smith
DSWA---------- Mr. Keith Weber
IRMC---------- Prof Paul Flanagan
ISS---------- LTC Barry Bryan
JLSC---------- Mr. Steve Strong
Joint Staff---------- Maj Tina Harvey
JSC---------- Mr. Rick Larson
NIMA---------- Mr, John Wood
NSA---------- Mr. H. Michael Greene
OATSDN(NCB)------ Mr. Tony Hermes
ODUSD(IA&IM)----- Mr. Jarnes Whittaker
OSIA---------- Ms. Bonnie Smith
US Air F'orce--------- Mr. John Colon
US ARMY---------- Mr. Charles jerzak
US NAVY---------- LCDR Eric Elser
USMC---------- LtCol Robert R. Logan

DISAIOMNCS Points of Contact

Personnel (Dl)---------- Mr, McAlphin
Programs (D2)---------- Mr. Mike Green
Operations (D3)---------- Mr.Ted Einersen
Logistics (D4)---------- Mr. Jim Robinson
Engineering (D6)---------- Dr. Fred Moxtey
Reqts Analysis &Integration (D7)---------- Mr. John Pelszynski
Modeling and Simulation(D8)---------- Dr. Ken Jo
DC---------- Mr. John Redding
DG---------- Ms. Lola DeGroff
DISA Europe---------- Lt Cot Paul Law
DISA Pacific---------- LTC Dennis Johnson
DITCO---------- Ms. Norma Hollansworth
JITC---------- LCDR Ann Bennett
OMNCS---------- Mr. Larry Wheeler
WESTHEM---------- Ms. Maitna Lampaziane

Other Contribntors

Mr. Tom Ainsworth
Mr. J.P. Angelone
Ma] Bill Barlow
Ms. Jt,lie Barrow
Lt Cot George Bettis
LTJG Mike Briggs
Ms. Sharon Campbell
Ms. Jeanette Carter
Mr. David Cathcart
CAPT Jim Day
Mr. Dave Dore
Mr. Roger Duncan
Maj Gregory Edwards
Mr. Ken Fagan
Dr. Barbara Falkner
Mr. Edward Fetzner
Ms. Susan Ficklin
Ms. Robin Frost
Mr. Hen Fullen
Mr. David Gaon
Maj Ralph Harris
Ms. Judawn Harvey
Mr. Michael Hutcheson
Mr. Bob Hutten
Mr. Ty Jackson
Mr. Henry Johnson
Mr. Paul Johnson
Ma] Bill Jones
Mr. John KaiKai
Dr. Prabba Kumar
Ms. Sharon Larson
Ms. Chris Long
LTC Martha Maurer
Ms. Ruby May
Mr. Dave McDonald
Mr. Robert Mintonye
Mr. Robert Molter
Maj Jeff Munn
Ms. Judith Naquin
Mr. Dave Norem
Mr. Gene Phillip
Ms. Deborah Phillips
Ms. C. Reberkenney
Mr. Russell Royston
Lt Cot David Scearse
Ms. Sanna Sims
Ms. Mary Slevin
Mr. Larry Spieler
Ms. Dee Ann Sullivan
Ms. Coaline Tippins
Ms. Rose Thomas
Mr. Ron Torezan
Mr. Gary Tucker
Mr. Bill Tufte
CMDR Jan Veneri
Mr. Larry Wheeler
Maj Rod Wilkinson

DII Master Plan Version 7.0 Production Team

Ms. Mary Rhoads
Cdr Mel Smith, RN
Dr. Mike McDonnell
Capt Byron Demby
Ms. Karen DeMeritte
Maj Kris Clifton
2Lt Victor Rios, Jr
Ms. Diana Smith

Team Leader: Mr. Len Tabacchi

FOREWORD

The Defense Information Infrastructure (DII) supports the Warfighter. The DII is a DOD and National asset. It is the sum of all information management assets owned by each of the Office of the Secretary of Defense (OSD) Principal Staff Assistants (PSAs), Joint Chiefs of Staff, Combatant Commanders, the individual Military Services, and Defense Agencies. The DII is not a single program, but a capability resulting from the integration of individual information management programs within the DOD.

The DII Master Plan is a tool for managing the DII evolution. It is a living, evolving document prepared through the combined efforts of OSD, the Joint Staff, the Military Services, and the Defense Agencies. The DII Master Plan is written from a DOD-wide perspective. It reflects the views of all owners, operators and users of the DII for achieving the Command, Control, Communications, Computers, and Intelligence For The Warrior (C4IFTW) Vision, and Joint Vision 2010 described further in section two of this plan.

The DII Master Plan is primarily a descriptive document. It is prescriptive only in that it reflects policy guidance stated elsewhere. The DII Master Plan provides the baseline description of DII policy, guidance, strategies, and initiatives. It is a management tool for identifying voids, overlaps, discrepancies, issues, and opportunities. These are addressed by the appropriate organizations.

Each version of the DII Master Plan will further refine this living document and will foster the ongoing collaborative process for focusing DOD-wide information technology efforts in support of combat and mission support forces.

TABLE OF CONTENTS

LIST OF FIGURES

SECTION 1

INTRODUCTION

1.1 Purpose

The Defense Information Infrastructure (DII) Master Plan establishes the common vision of the DII for the Department of Defense (DOD). It defines and describes the major elements of the DII to facilitate the effective management and evolution of the DII. The DII Master Plan assists in collaborative planning across the DOD to ensure that the right resources are programmed to do the right things, at the right time, by the right organizations; and to facilitate identifying DII voids, discrepancies, issues, and opportunities. As such, the DII Master Plan provides a road map for the migration and implementation of DII elements, and describes initiatives that eliminate the shortfalls in the current DII.

1.2 Overview

The body of the document (Sections 1 through 4) provides a high-level overview of the DII. Section 1 provides a brief introduction, major differences from the previous version, and how to obtain copies. Section 2 provides general information on the DII. It defines and scopes the DII; characterizes the architectural context and interdependencies among elements of the DII; highlights some of the key policies, strategies, and plans related to the DII; and discusses the technology direction to be used to evolve the DII. Section 3 describes specifics about the DII as a whole, in the same format used in the appendices. This includes: baseline description, roles and responsibilities, requirements and objective environment, strategy, near-term programs and initiatives, schedule, interdependencies, performance measures, references, related working groups, and office of primary responsibility. In addition, there is a high-level paragraph on resources drawn from the TAB-G annex to the Services' and Defense Agencies' FY 99-2003 Program Objective Memorandum. Additional detail is not presented in the appendices because the funding information is considered sensitive for individual DII elements.

The appendices contain a greater level of detail for each major DII element. The structure of the appendices follows the framework of the DII Elements depicted in Figure 2.4-1 and at the introduction to the appendices. Each appendix begins with an overview describing the applicable DII elements and interdependencies with other appendices.

Appendix A (Communications and Computer Infrastructure) addresses the communications and computing infrastructure elements used at the enterprise, base, and deployed/afloat locations of the DII. Appendix B (Common Computing and Communication Applications (from hereon referred to as "Common Applications")) describes the computing and communications products and services available to all functional areas and organizations; e.g., messaging, electronic commerce/electronic data interchange. Appendix C (Foundation: Program and Technical Activities) describes the common policies, technologies, standards, services, and tools that comprise the foundation for the other DII elements. Appendix D (Functional Area Applications) describes the application software used by functional communities such as command and control, intelligence, surveillance and reconnaissance, acquisition, logistics, finance, personnel, medical, and reserves. It is intended that all functional areas be included in Appendix D. It is

also understood that some functional area applications are considered "systems" (e.g., Global Command and Control System (GCCS)) and as such have components that are reflected in other elements of the DII. However, we have placed these in the Functional Area Applications appendix because the systems "run" functional applications.

1.3 What is new in Version 7.0

The first version of the DII Master Plan was published in November 1994. Subsequent versions have added additional information and incorporated Service and Agency comments and contributions.

Major emphasis in Version 7.0 has been on improving the content of schedule, interdependencies, and performance measures subparagraphs for the DII and each DII element. In addition, the following updates have been made:

Major Rewrites:

- **Section 2 - DII-General.** Reflects the most recent National Military Strategy and the Defense Reform Initiative report. It describes the relationship the Joint Vision 2010, C4IFTW, DOD ITM Strategic Plan, Service Strategies, and the DII Master Plan. It also describes the relationship among key technical guidance documents including the C4ISR Architectural Framework, the TAFIM, and Joint Technical Architecture. The discussion of the Strategic Technical Guidance was deleted.

- **Section 3 - DII Specific**. Includes an updated description of performance measures based on the ITM Strategic Plan. It includes new information on Defense Integration Support Tool, key councils overseeing aspects of the DII, and descriptions of some innovative contract vehicles for acquiring technical services.

- **Section 4 - Voids, Discrepancies, Issues and Opportunities**. Added issue on identifying need for clear DOD architecture policy and need to rationalize the overlaps between the C4ISR Architecture Framework, TAFIM, JTA, and DII COE. Other new issues for resolution include: requirement for ATM standards, a new section addressing the DOD IT workforce, and another new section addressing interoperability with the information infrastructures of coalition partners.

- **C.5 - Architecture.**

- **D.2.1.6 - Systems Engineering.**

- **D.2.1.9 - Installations**.

- **D.2.5 - Health Affairs**.

- **D.2.6 - Finance.**

Other Changes:

- Appendix A.2 DII Computing Infrastructure. This section includes a new introductory sub-section highlighting the three-tiered DII computing infrastructure and provides guidelines for use of the different tiers. It also introduces the concept of Regional Support Centers to provide customers with local information technology services on a customer-driven, cost-reimbursable, self-sustaining basis.

- A.4.2: U.S. Navy. This section was updated to include IT 21 capabilities.

- B.1: Defense Message System. Improved descriptions in the schedule and interdependencies sections.

- B.2: Electronic Commerce. Added information on the new Joint Electronic Commerce Program Office.

- B.5: Information Dissemination Management. Expanded the Information Dissemination Management section to address requirements and the objective environment, strategy, and improved the descriptions of near-term programs, initiatives, and schedules.

- C.10: Information Assurance. Scheduling and interdependency information were improved. This section was moved from the Appendix on Common Applications (Appendix B) to the Appendix on Program and Technical Activities (Appendix C) to be consistent with the current POM TAB-G instructions.

- D.1.2: Theater/Tactical C2 Applications. This section was deleted. This section has been superceded by the GCCS, GCSS, and the Base and Deployed/Afloat Communications and Computer Infrastructure sections now contained in Section A.4.

- Change bars were left in the document to allow quicker identification of new material.

- DII Master Plan is being distributed in CD-ROM format in accordance with recommendations in the Defense Reform Initiative. (See Paragraph 1.4 below.) It is produced using MS Office 97.

1.4 Getting a Copy of the DII Master Plan

As of the date of publication, the Director, Defense Information Systems Agency (DISA) has determined that distribution of the DII Master Plan will be limited to U.S. Government personnel and their support contractors. For this reason the DII Master Plan has not been made available on the Internet. U.S. Government personnel can obtain copies of the DII Master Plan, either in paper or on CD-ROM, through the Defense Technical Information Center (DTIC), by contacting Ms. Karen DeMeritte at (703) 607-4223 or DSN 327-4223, via electronic mail at demeritk@ncr.disa.mil or at:

Defense Information Systems Agency
Plans Division (D52)
701 South Courthouse Road
Arlington, VA 22204-2199

DOD support contractors can obtain a hard copy from DTIC:

Defense Technical Information Center
8725 John King Road, Suite 0944
Ft. Belvoir, VA 22060-6218

SECTION 2

DII--GENERAL

2.1 Purpose

In December 1992, DOD recognized that the new warfighting context required a new approach to information systems. Defense Management Report Decision (DMRD) 918C created the DII not as a single program, but as a capability resulting from the integration of individual information management programs across the DOD to: (1) revolutionize information exchange Defense-wide, (2) strengthen our ability to apply computing, communications, and information management capabilities effectively to the accomplishment of DOD's mission, (3) significantly reduce the information technology burdens on operational and functional staffs, and (4) enable the operational and functional staffs to access, share, and exchange information world-wide with minimal knowledge of communication and computing technologies. Simply put, the DII is to provide seamless, secure information products and services to DOD users, especially warfighters, in support of decision making and mission accomplishment.

2.2 Definition

The DII is the web of communications networks, computers, software, databases, applications, weapon system interfaces, data, security services, and other services that meet the information processing and transport needs of DOD users, across the range of military operations. It encompasses: (1) sustaining base, tactical, DOD-wide information systems, and Command, Control, Communications, Computers, and Intelligence (C4I) interfaces to weapons systems, (2) the physical facilities used to collect, distribute, store, process, and display voice, data, and imagery; (3) the applications and data engineering tools, methods, and processes to build and maintain the software that allow Command and Control (C2), Intelligence, Surveillance, Reconnaissance, and Mission Support users to access and manipulate, organize, and digest proliferating quantities of information; (4) the standards and protocols that facilitate interconnection and interoperation among networks; and (5) the people and assets which provide the integrating design, management and operation of the DII, develop the applications and services, construct the facilities, and train others in DII capabilities and use.

2.3 Scope

The DII includes the information infrastructure of the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff (CJCS), the Defense Agencies, and the Combatant Commands. The DII includes information infrastructure regardless of its role or location, whether it is part of the enterprise infrastructure, the sustaining base, deployed, or afloat. The information interfaces to industry, government, academia, and our allies are also within the scope of the DII as are weapons systems interfaces to the DII. Figure 2.3-1, DII Architecture Concept, further illustrates the scope of the DII.

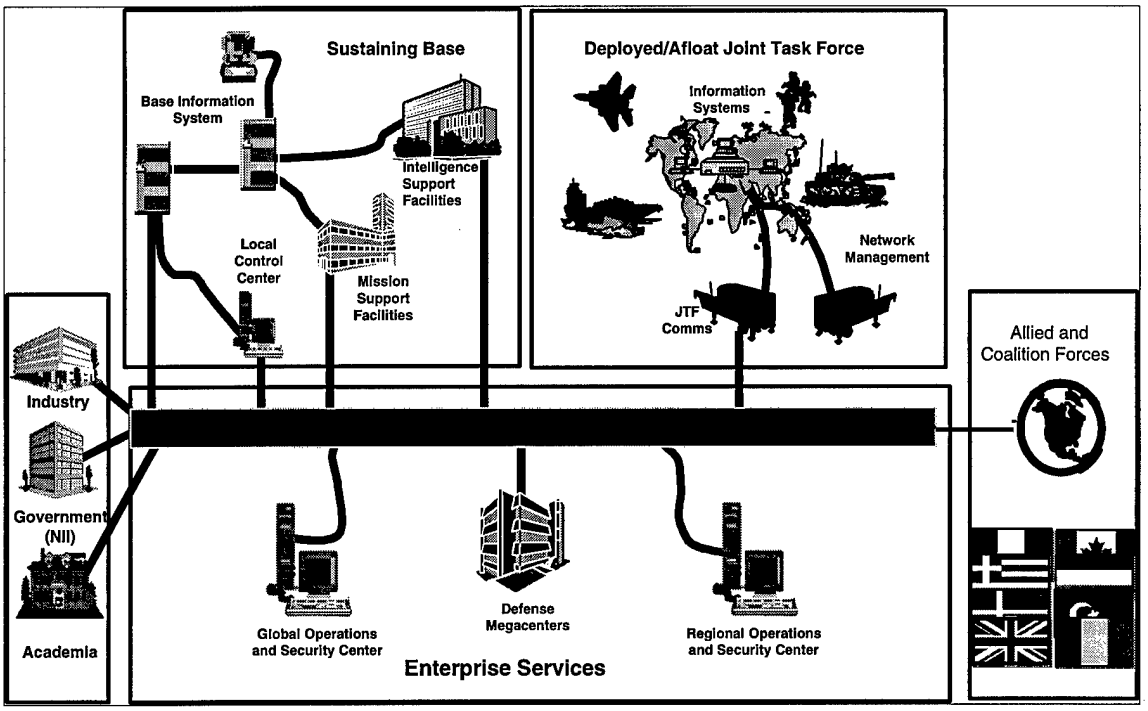


Figure 2.3-1. DII Architecture Concept

2.4 Description

The DII provides information products and services for the Combatant Commands, Military Services, and Defense Agencies. The DII is made up of many elements and the major ones are shown in Figure 2.4-1 on the following page. Each major element of the DII is connected, much like the pieces of a puzzle. And, like a puzzle, the DII is not complete without every piece. No single piece is meaningful when it is separated from the rest, but a single missing piece will affect the whole picture.

2.4.1 Foundation: Program and Related Technical Activities

These activities provide life-cycle support to all elements of the DII. These activities include requirements gathering, modeling and simulation capabilities, continual assessment of new technology, information transport and processing standards, testing and evaluation, modern software engineering practices, sound architecture and policy. Information Assurance products and services ensure information availability, provide protection from unauthorized access and disclosure, and response to attacks. Further discussion of the Foundation: Program and Related Technical Activities can be found in Appendix C.

2.4.2 The Communications and Computer Infrastructure

The Communications and Computer Infrastructure of the DII provides information processing and transport services used by Functional Area Applications and Common Applications. It includes the Defense Information System Network (DISN) for information transport; the Defense Megacenters for information system processing; the DII Control Centers that manage the DII network and systems; and Base and Deployed/Afloat Communications and Computer

assets. Together, these elements form DOD's end-to-end capability for information distribution, processing, storage, and display. The DII Control Centers, operated cooperatively by DISA, the Military Services and Defense Agencies provide Global, Regional, and Local Control Centers to manage the Communications and Computer Infrastructure. Further discussion of the Communications and Computer Infrastructure elements of the DII can be found in Appendix A.

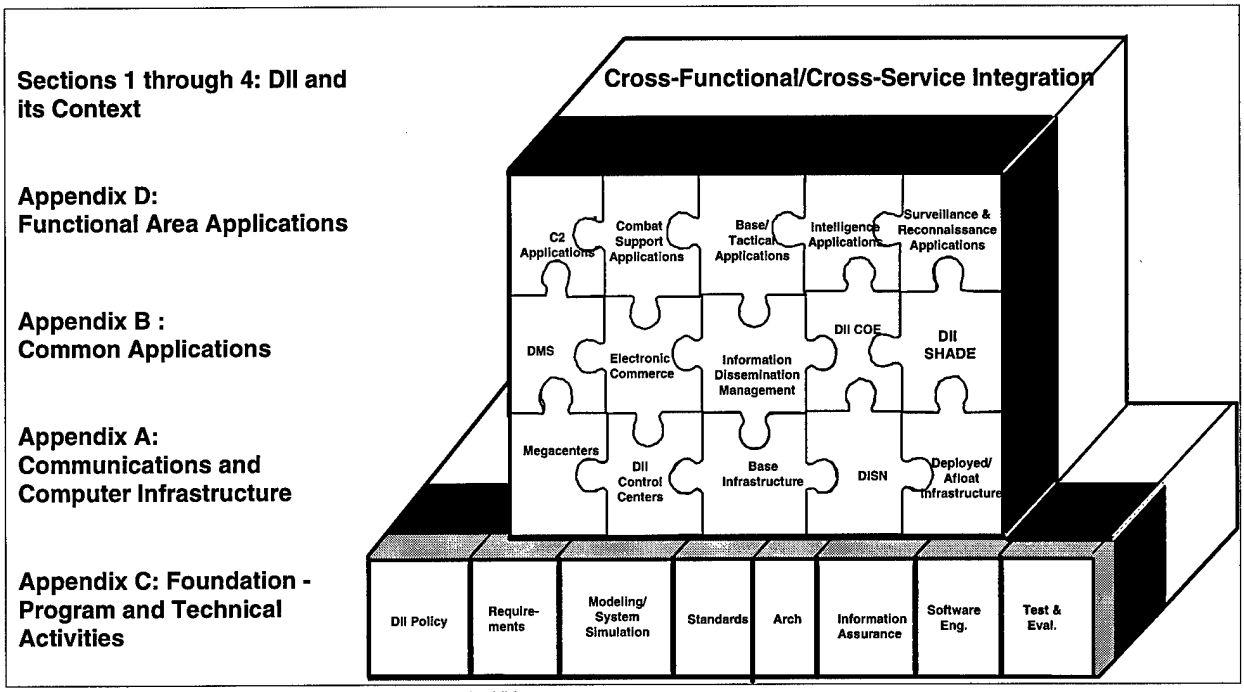


Figure 2.4-1. The Elements of the DII

2.4.3 Common Applications

Common Applications provide cross-functional, cross-organization capabilities for personal and organizational messaging through the Defense Message System (DMS), and support electronic commerce (e.g., procurement, provisioning, shipping, making payments) through Electronic Commerce/Electronic Data Interchange (EC/EDI). The DII Common Operating Environment (COE) provides for integrated common support services, a corresponding software development environment for functional applications, and enables execution and integration of Joint and Military Service mission applications. The Shared Data Environment (SHADE) supports interoperability of Functional Area Applications at the data level among Military Services and functional areas as needed to conduct DOD's mission. The Information Dissemination Management Initiative will coordinate the dissemination of information by the NCA as a key function within the DII. Further discussion of the Common Applications elements of the DII can be found in Appendix B.

2.4.4 Functional Area Applications

Functional Area Applications include all DOD mission areas: C2 (e.g., Global Command and Control System (GCCS)) including tactical applications, and combat support applications (e.g., the Depot Maintenance System and Global Combat Support System (GCSS)). Functional Area

Applications depend upon Common Applications to provide the environment for sharing information among functional communities. Functional Area Applications also rely upon the information processing and transport capabilities of the Communications and Computer Infrastructure to deliver service to their functional communities. Further discussion of the Functional Area Applications can be found in Appendix D.

2.5 Key Related Strategies, Guidance, Policies, Plans, and Significant Reports

As Figure 2.5-1 shows, there are a number of strategies, guidance, policies, and plans on which the DII is related or dependent. The following subparagraphs discuss some of the key documents and their relationship to the DII.

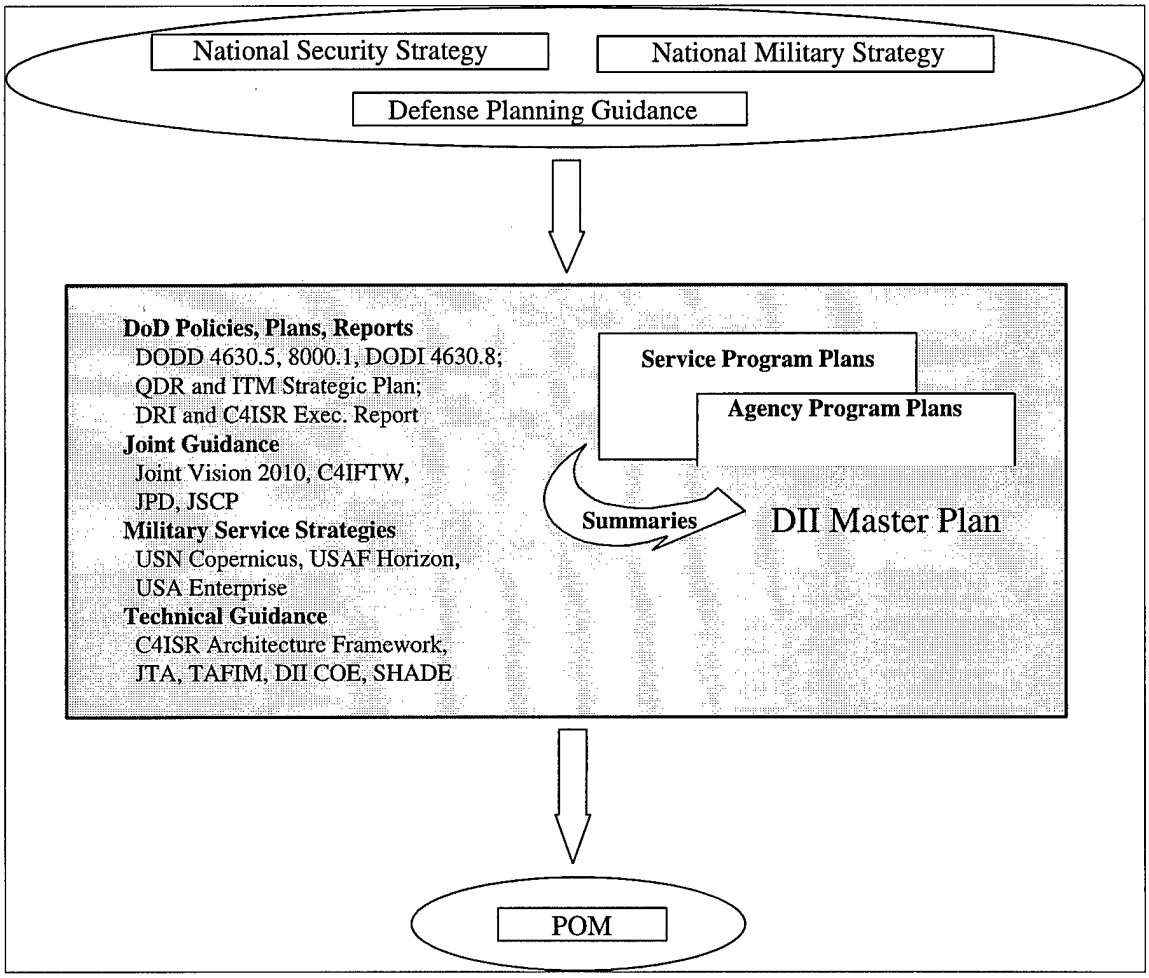


Figure 2.5.-1. Relationship of Key Strategies, Guidance, Policies, Plans, and Reports

2.5.1 DOD Strategies and Guidance

Evolution of the DII has been driven by high-level policy and guidance from OSD and the CJCS; by the warfighter requirements; by Military Service strategies, and technical guidance.

2.5.1.1 The National Military Strategy

> "The remarkable leverage attainable from modern reconnaissance, intelligence collection and analysis, and high-speed data processing and transmission warrants special emphasis. The Services and Combatant commands require fused information systems. These systems enhance our ability to dominate warfare. We must assure that this leverage works for us and against our adversaries." - General John M. Shalikashvili, CJCS

The National Military Strategy, "Shape, Respond, Prepare Now -- A Military Strategy for a New Era," is illustrated in Figure 2.5.1.1-1. It prescribes the tailored employment of military capabilities in peace and the use of decisive military force in war to achieve our national military objectives in the new international environment.

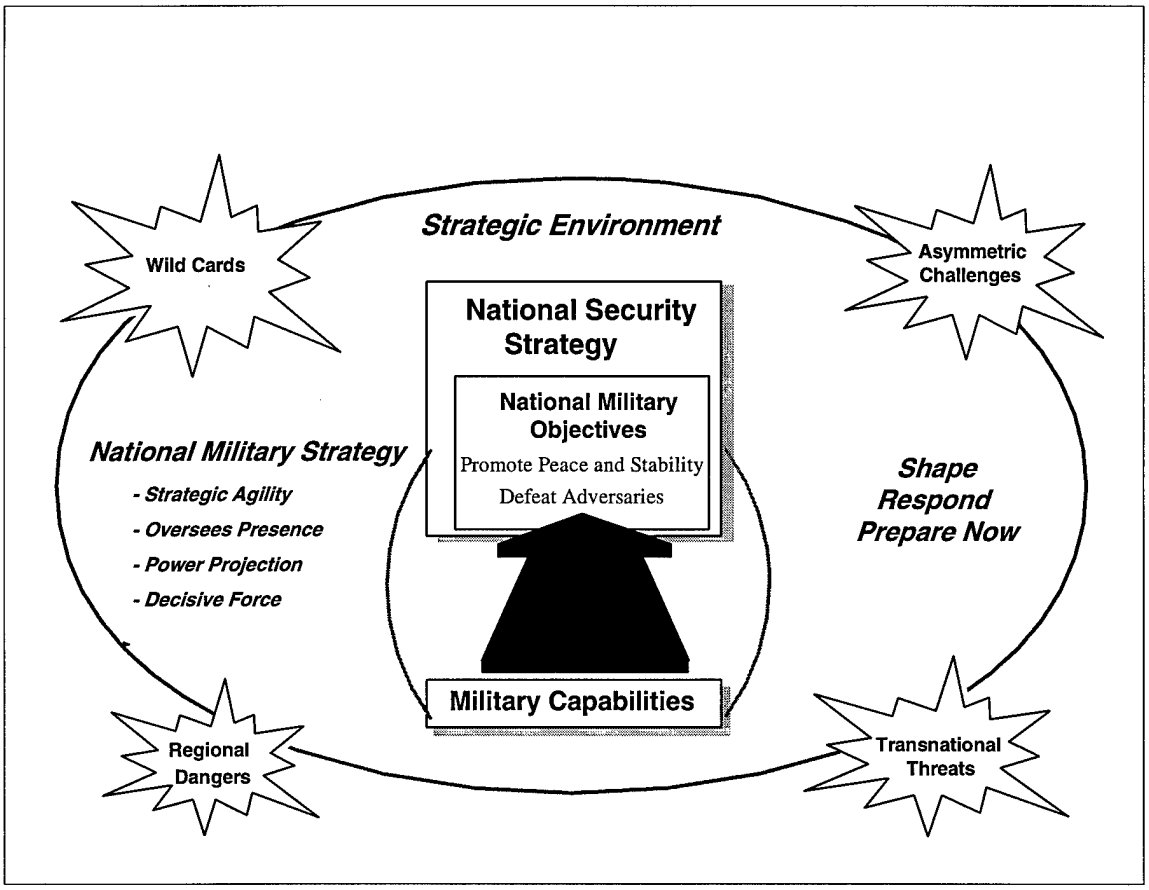


Figure 2.5.1.1-1. National Military Strategy

The National Military Strategy relies on power projection by highly flexible, rapid response, tailored force packages under Joint Task Force (JTF) or Combined Task Force (CTF) command. These force packages will support a spectrum of military and political responses to promote national interests worldwide. The National Military Strategy dictates that U.S. forces will be structured to project power from Continental United States (CONUS) bases, sanctuary locations, and in-theater locations to an area conflict anywhere in the world.

The environment of future military operations includes:

- Regional orientation
- Nontraditional, transnational, and unpredictable threats
- Ad-hoc coalitions and/or unilateral operations
- Adaptive planning and strategic agility
- Smaller total force - reduced forward presence
- Rapid response capability
- Operations other than warfighting (e.g., peacekeeping, sanctuary, etc.)
- Asymmetric risks: terrorism, proliferation of weapons of mass destruction, and information warfare
- Tailored force packages deployed under JTF or CTF command
- Reduced funding

2.5.1.2 Defense Planning Guidance (DPG) and Joint Strategic Planning System (JSPS)

The DPG and JSPS planning documents are used by the Secretary of Defense (SECDEF) and the CJCS respectively to guide the Military Services and Defense Agencies in building their Program Objective Memorandums (POMs). These documents call for consolidating redundant functions, increasing overall system throughput, merging existing "stovepipe" systems to achieve interoperability and enabling Joint tactical commanders to control component forces better. The DPG Fiscal Year (FY) 1998-2002 stated:

> "... the Department is developing a 'global infosphere' designed specifically to support all combat functions and combat support functions with an unconstrained information flow through air, land, sea, and space. This global infosphere will be based on C4I for the Warrior (C4IFTW) principles [See paragraph 2.5.3.3], and implemented through the Defense Information Infrastructure (DII) initiative...."

2.5.2 DOD Policies, Plans, and Reports

2.5.2.1 DOD Policies

Although the term "DII" has been used since 1992, there is no published DOD policy which specifically defines the DII. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD(C3I)) recently formally coordinated DOD Directive 4630.5, "Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems;" and DOD Instruction 4630.8, "Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems." Additionally, DOD Directive 8000.1, "Defense Information Management (IM) Program, is undergoing revision. The draft revisions expand the scope of these documents beyond C3I systems to include all functional areas. They also fill the policy voids concerning the DII definition and interoperability responsibilities.

Policies related to the DII are described in Appendix C.1.

2.5.2.2 Report of the Quadrennial Defense Review (QDR)
(www.dtic.mil/defenselink/pubs/qdr)

The QDR, completed in May 1997, followed a path that led from threat, to strategy, to implementation, and finally to resource issues. The QDR determined that the information revolution is creating a Revolution in Military Affairs (RMA) that will fundamentally change the way U.S. forces fight. They further determined that we must exploit these and other technologies to dominate in battle, and to use Joint Vision 2010 as the template.

The QDR serves as the overall strategic planning document of the DOD and is intended to fulfill the strategic planning requirements of the Government Performance and Results Act (GPRA) of 1993, Public Law (P.L.) 103-62.

The QDR cites as one of the critical enablers: "Our global communications must allow for the timely exchange of information, data, decisions, and orders, while negating an adversary's ability to interfere in our information operations. The ability to gather, process, and disseminate an uninterrupted flow of reliable and precise information anywhere in the world and under any conditions is a tremendous strategic and military advantage. These capabilities, when combined with the ability to protect one's own information systems and at the same time negate an adversary's, result in information superiority." The QDR goes on to state that critical to ensuring that ability will be institutionalization of information operations; i.e., the integration of information operations concepts into military planning, programming, budgeting, and operations. In the context of Joint Vision 2010, DOD will continue to develop additional guidance to strengthen information assurance - the protection, integrity, and availability of critical information systems and networks. Further, the DOD will allocate adequate resources for these efforts within information technology investment programs and improve the Defense-wide planning and implementation process, regularly assessing funding adequacies for all information assurance program components.

2.5.2.3 DOD Information Technology Management (ITM) Strategic Plan
(www.dtic.mil/c3i/cio)

DOD ITM Vision: Information superiority achieved through global, affordable, and timely access to reliable and secure information for worldwide decision-making and operations.

The Federal Information Technology Management Reform Act (ITMRA) of 1996, P.L. 104-106, Division E, commonly called the Clinger-Cohen Act, became effective 8 August 1996. The SECDEF designated the ASD(C3I) as the DOD Chief Information Officer (CIO). The ITM Strategic Plan, Version 1.0, dated 20 March 1997, provides IT guidance to the DOD to comply, and aligns with the QDR and Joint Vision 2010. Version 2.0 is scheduled for publication by late Spring.

The Plan establishes the following goals:

1. "Become a mission partner" - to focus on mission support.
2. "Provide services that satisfy customer information needs" - to focus the information infrastructure on customer, information, service, and performance.
3. "Reform IT management" - to highlight initiatives to streamline DOD policies and procedures.
4. "Provide information assurance...." - to expedite implementation of information security practices and capabilities.

Goal 2 applies directly to the DII, including desired outcomes and outcome performance indicators. The following extracts portray future DII directions and the specific role of the DII Master Plan in support of the DOD ITM Strategic Plan:

> "The DII Master Plan identifies the major elements of the information infrastructure, roles and responsibilities, and serves as a tool to track the evolution of the DII into a service environment. To meet its global mission, DOD must focus the information infrastructure on getting information to mission and mission support customers from multiple information suppliers/providers. Today's systems are too often narrowly focused, not fully interoperable, and support a single function or organization requiring users to assemble information from incompatible sources. As information generation capabilities become more complex (e.g. maps, pictures, correspondence) DOD must begin to manage the information space for the user, and integrate and modernize its information infrastructure. Users need "navigation" services to leverage new technologies and information resources to retrieve, fuse and format information quickly. Accelerating the establishment of a network of shared databases and focusing the use of Internet technologies will support the ability of users to get information they want and reduce redundancies in stovepiped systems. A common operating environment throughout DOD from installations to weapon system platforms will expedite application system implementation and allow incremental implementation. Infrastructure components must move from an "organization/technology centric" paradigm to an interconnected set of services/products with quantifiable cost and performance measures to determine value-added to the mission."

A persistent theme throughout the DOD ITM Strategic Plan is an emphasis on performance measures and accountability to mission/operations support to on-base commands and tactical units. The DII Master Plan provides the central, comprehensive description of all elements of the DII, strategic objectives, and associated performance measures (See paragraph 9 in each section of the DII Master Plan appendices.). This information will contribute to a comprehensive DII simulation model to demonstrate, train, and analyze alternative improvements.

A DEPSECDEF memorandum dated 2 Jun 1997, subject: "Implementation of Subdivision E of the Clinger-Cohen Act of 1996 (Public Law 104-106)" gives further guidance on how the DOD

will implement the ITMRA. Attachment 1 to the memo assigns responsibilities to the ASD(C3I) as the DOD CIO. Attachment 2 is the charter for the DOD CIO Council.

2.5.2.4 Defense Reform Initiative Report (DRI)

(www.defenselink.mil/pubs/dodreform)

In November 1997, the Secretary of Defense published the Defense Reform Initiative Report. Its goal is to ignite a revolution in business affairs within the DOD that will bring to the Department management techniques and business practices that have restored American corporations to leadership in the marketplace. In order to rid the defense establishment of Cold War structures and practices and achieve fundamental reform in how the DOD conducts business, the report presents a series of initiatives in four major areas:

- Reengineer: Adopt modern business practices to achieve world-class standards of performance. Some initiatives include instituting a paper-free contracting process for major weapons systems by 1 January 2000; creating paper-free systems for weapons support and logistics; shifting to the use of electronic catalogues and electronic "shopping malls"; and ending volume printing of all DOD-wide regulations and instructions by 1 July 1998 after which they will be available only on the Internet or CD-ROM.

- Consolidate: Streamline organizations to remove redundancy and maximize synergy. Some changes include reductions in the OSD staff, Defense Agencies, DOD Field Activities and the Joint Staff Activities; and establishment of a Defense Management Council to serve as the Board of Directors for the Defense Agencies and to oversee the continued reengineering of the DOD.

- Compete: Apply market mechanisms to improve quality, reduce costs, and respond to customer needs.

- Eliminate: Reduce excess support structures to free resources and focus on core competencies.

2.5.2.5 Command Control Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Executive Summary Report

In October 1995, the Deputy Secretary of Defense directed the DOD to improve the means and processes for meeting the C4ISR needs of warfighters. The ASD(C3I) formed a C4ISR Integration Task Force (ITF) to address integration and interoperability from a broader perspective and at a higher level than any previous effort.

C4ISR work has served to validate and expand the C4I for the Warrior (C4IFTW) vision discussed in section 2.5.3.3. C4ISR provides the ASD(C3I) with an architectural and programmatic framework for integrating and rationalizing the communications and computing infrastructure that supports the functional areas of command and control, intelligence, surveillance, and reconnaissance for which the ASD(C3I) is responsible.

In August 1996, the C4ISR ITF established a Defense-wide C4ISR strategic vision and made major recommendations for improving the means and processes that deliver C4ISR capabilities. The products of the C4ISR ITF include the definitions of architecture and interoperability terms, a C4ISR Architecture Framework focusing on Operational and Systems Architectures (See Appendix C, Paragraph 5), and a Joint Technical Architecture (JTA) (See OSD memo, "Implementation of the DOD Joint Technical Architecture," dated Aug 22, 1996, and home page: www-jta.itsi.disa.mil) for use in all C4I systems development, upgrade, and integration.

C4ISR ITF recommendations include:

- Create and maintain a C4ISR Strategic Plan
- Implement a common approach for architecture
- Strengthen the policy for Compatibility, Interoperability, Integration and Security
- Determine the feasibility of a Systems Integration Management process
- Implement a standardized, mission oriented approach to requirements definition
- Create an integrated, nested set of requirements from top to bottom
- Strengthen linkages among JSPS, requirements, and PPBS processes
- Align defense resources with joint requirements and priorities
- Consider evolutionary and other non-traditional acquisition methods for C4ISR
- Create a comprehensive management planning process
- Create a knowledge base with integrated tool sets
- Educate and train the workforce

In addition, DOD has undertaken a C4ISR Mission Assessment (CMA) to develop a C4ISR objective system architecture and investment strategy. The CMA's efforts are linked to ongoing force/weapons mix studies: Deep Attack Weapons Mix, Joint Suppression of Enemy Air Defenses, Close Support End-to-End Assessment, and Theater Air and Missile Defense Studies - focusing on performance impacts and new concepts enabled by future C4ISR capabilities.

2.5.3 Joint Guidance

2.5.3.1 Joint Vision 2010

> "The nature of modern warfare demands that we fight as a joint team. This was important yesterday, it is essential today, and it will be even more imperative tomorrow. Joint Vision 2010 provides an operationally based template for the evolution of the Armed Forces for a challenging and uncertain future. It must become a benchmark for Service and Unified Command visions."
>
> General John M. Shalikashvili, CJCS

Joint Vision 2010 is the conceptual template for how America's Armed Forces will channel the vitality and innovation of our people and leverage technological opportunities to achieve new levels of effectiveness in Joint warfighting.

VISION 2010: America's Military Preparing for Tomorrow: Quality People Trained, Equipped and Ready for Joint Operations

- *Persuasive in Peace*
- *Decisive in War*
- *Preeminent in Any Form of Conflict*

This vision of future warfighting embodies the improved intelligence and command and control available in the information age and goes on to develop four operational concepts depicted in Figure 2.5.3.1-1: dominant maneuver, precision engagement, full-dimensional protection, and focused logistics.

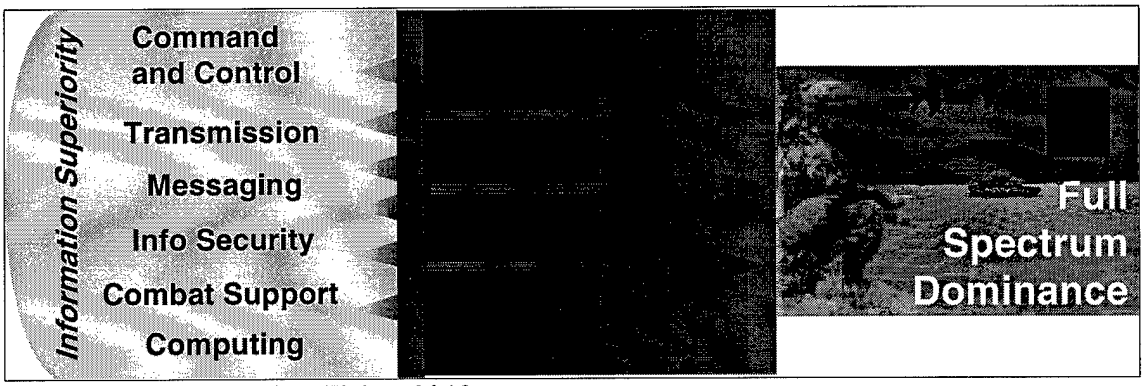


Figure 2.5.3.1-1. Joint Vision 2010

Full Spectrum Dominance (the full range of military operations from humanitarian assistance, through peace operations, up to and into the highest intensity conflict) will be the key characteristic we seek for our Armed Forces in the 21st century.

Joint Vision 2010 emphasizes that Full Spectrum Dominance is dependent on information superiority, that is, the capability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Instead of relying on massed forces and sequential operations, we will achieve massed effects in other ways. Information superiority in combination with higher lethality weapons will allow us to conduct attacks concurrently that formerly required massed assets applied in a sequential manner. Commanders will be able to achieve the necessary destruction or suppression of enemy forces with fewer systems thereby reducing the need for time-consuming and risky massing of people and equipment.

As we move toward Joint Vision 2010, we move toward a common goal, that is, a Joint force--persuasive in peace, decisive in war, preeminent in any form of conflict.

2.5.3.2 Joint Vision 2010 Implementation Master Plan (Draft)

The purpose of this Joint Vision 2010 Implementation Master Plan is to focus and integrate efforts to assess Joint Vision 2010 concepts and desired operational capabilities. When published, this plan will provide direction on implementation, project management, long range planning, and establishes detailed assessment roadmaps. The draft plan, CJCSI 3010.02, dated 9 January 1998, is undergoing DOD-wide review.

2.5.3.3 Command, Control, Communications, Computer, and Intelligence for the Warrior (C4IFTW)

Joint Vision 2010 provides an operationally based template for the evolution of the Armed Forces for a challenging and uncertain future. C4IFTW is subordinate, thoroughly supportive, and perfectly aligned to Joint Vision 2010. By achieving the C4IFTW vision, we will provide the information superiority needed for the operational concepts under Joint Vision 2010.

The vision of C4IFTW is to provide an accurate and timely common operational picture. This view is provided through a widely distributed and robust user-driven infrastructure into which the warrior "plugs in", as illustrated in Figure 2.5.3.3-1. The three disciplines critical to the Warfighter are C2, Intelligence, and Mission Support. This information for the Warfighter -- whether in the air, on land, at sea -- must be secure and accessible through computer and communications systems.

C4IFTW Vision: The Warrior needs a fused, real-time, true picture of the battlespace and the ability to order, respond, and coordinate vertically and horizontally to the degree necessary to prosecute the mission in that battlespace.

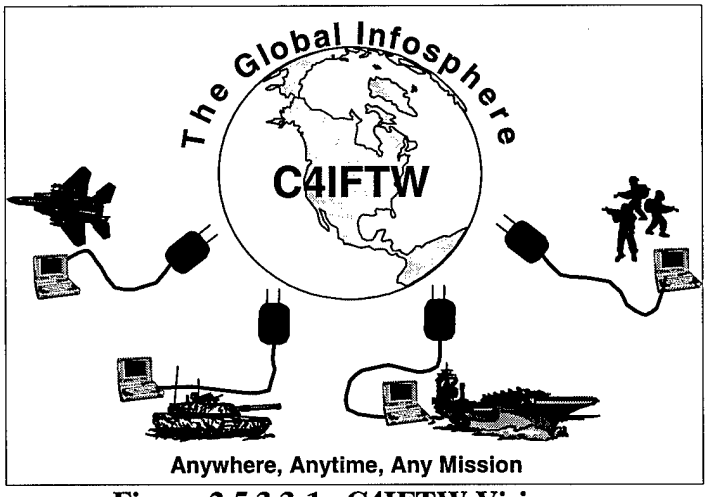


Figure 2.5.3.3-1. C4IFTW Vision

The global information infrastructure must respond quickly to new joint, coalition, and organizational relationships created on demand. Senior decisionmakers will continue to require accurate, immediate, reliable information to maintain a safe, credible, global deterrent against the

use of weapons of mass destruction. Three key information systems capabilities are needed to achieve the C4IFTW vision:

- Split Base/Reach Back - The ability to supplement the Warfighters' limited mission support staff with forces "deployed" to the battlespace by electronic means.

- Same "Look and Feel" - The information systems will interact with Warfighters the same when in garrison and in the battlespace.

- Tailored C4I Information – The Warfighter chooses the types of information to be "pushed" forward and "pulled" when needed. Real-time battlespace information is the result of fusing Preplanned Essential Elements of Information, over-the-air updating, and warrior pull on demand. Information is correlated, prioritized, and clearly presented according to human factors design principles.

2.5.4 Military Service Strategies

The Military Services have developed information system strategies complementary to Joint Vision 2010 and C4IFTW. The Military Service strategies support normal and contingency warfighting capabilities in line with OSD and CJCS policy. They include:

- The Navy is moving toward implementing Information Technology 21. This builds on the Navy's Copernicus Architecture. Copernicus puts the tactical commander at the center controlling information flow to support mission execution through information-pull rather than producer-push. Four pillars tie together the commander afloat, the JTF, the numbered fleet commander, and the CINC ashore: (1) Global Information Exchange System; (2) CINC Command Complex; (3) Tactical Data Information Exchange Systems; (4) Tactical Command Center.

- The Army's Enterprise Strategy provides a view of the Army's information needs as a Military Department, as a component of the fighting force, and as the sustaining force for C/JTF operations. The Enterprise vision enhances Information Mission Area (IMA) and non-IMA community understanding. The implementation plan provides guidance to the IMA community and helps influence program planning and budgeting.

- The Air Force Horizon Strategy provides the warfighter with responsive advanced C4I systems services. It provides reliable, high bandwidth, cost-effective, mission-oriented C4I systems to user-focused programs such as Combat Information Transport System, BIP, NCCs, GCCS, and Theater Battle Management Core System. It supports the Joint Staff C4IFTW concept which emphasizes joint interoperability objectives, derived from Joint operational requirements.

- The Marine's approach to tactical command and control is three-fold. The Marine Air Ground Task Force Command, Control, Communications, Computers and Intelligence (MAGTFC4I) System provides a common suite of software applications developed on the Joint Marine Corps Information System (JMCIS) Unified Build that includes Tactical Combat Operations (TCO), Amphibious Planning Tool (APT), and Intelligence Analysis

System (IAS). A total of twenty-six applications are planned for MAGTF C4I. The Marine Corps Common Hardware Suite provides a suite of standard computer platforms to support the software applications. The Tactical Data Node (TDN) and the Digital Technical Control (DTC) provide a common information transfer system and digital technical control.

Military Service Communications and Computer Infrastructure initiatives are described in Appendix A.

2.5.5 Technical Guidance

The discussion below summarizes the current DII architectures guidance. For additional information, see the architecture policy issue in Paragraph 4.1 and additional discussion on DOD architectures in Appendix C.5.

2.5.5.1 C4ISR Architecture Framework

The Version 2.0 of the Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) Architecture Framework was approved by the Architecture Coordination Council on 23 February 1998. The policy memorandum signed by the USD(A&T), the acting ASD(C3I) and the Joint Staff (J6) directs that all on-going and planned C4ISR architectures be developed in accordance with Version 2.0 of the Framework. Existing C4ISR architectures will be redescribed in accordance with the Framework during appropriate revision cycles. The C4ISR Framework defines three types of architectures: Operational, Systems and Technical. Operational Architectures are used to identify and document operational requirements by describing the tasks and activities, operational elements, and information flows required to accomplish or support a military operation. A Technical Architecture is the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements. A Technical Architecture includes a collection of standards, conventions, rules and criteria organized into profiles that govern system services, interfaces, and relationships. A Systems Architecture associates physical resources and their performance attributes to the Operational Architecture and its requirements per standards defined in the Technical Architecture.

The C4ISR Architecture Framework defines a common approach for the Military Services, Unified Commands, and Defense Agencies to follow in developing operational, technical, and systems architectures. The Framework provides guidelines and defines a process that can be used across DOD for developing C4ISR operational, technical, and systems architectures with a focus on support to the warfighter. Although developed as a means for describing C4ISR operational, technical and systems architectures to support warfighting tasks, the Framework can be readily extended to other functional areas such as finance, personnel, and acquisition.

2.5.5.2 The Joint Technical Architecture

Definition: The JTA is the technical architecture component of C4ISR Architectural Framework. The JTA specifies a common set of mandatory information technology standards and guidelines to be used in all new and upgraded C4I acquisitions across the DOD. The JTA

draws on the TAFIM, which provides general guidance and documents the processes and framework for defining the JTA and other technical architectures. The JTA necessarily includes requirements as related to interoperability by identifying the minimum set of standards. As the JTA evolves, the nature and relationship to the standards information in the TAFIM (particularly Volume 7) will evolve.

Scope: The current version of the JTA applies to all C4I systems and the interfaces of other key assets (e.g., weapons systems, sensors, office automation systems, etc.) with C4I systems. The JTA also applies to C4I Advanced Concept Technology Demonstrations and other activities that lead directly to the fielding of operational C4I capabilities. The JTA will be used by anyone involved in the management, development, or acquisition of new or improved C4I systems within DOD. Future versions of the JTA will extend the Version 1.0 scope from C4I Systems to include information technology in all DOD systems. For additional information, see Appendix C.5 and http://www-jta.itsi.disa.mil.

2.5.5.3 Technical Architecture Framework for Information Management (TAFIM)

Prior to the C4ISR Architecture Framework and the JTA, the primary DOD guidance specifically focused on architectures was the TAFIM. Use of the TAFIM is mandated under DODD 5000.1 for new systems and major system upgrades. The overlap that exists among the TAFIM, C4ISR Architectural Framework, and the JTA must be rationalized and a clear set of guidance provided on their use (See Section 4.1). The TAFIM volumes noted below continue to provide critically needed technical guidance to the Department.

- **Technical Reference Model (TAFIM VOL 2):** The purpose of the Technical Reference Model described in this document is to provide a common conceptual framework, and define a common vocabulary so that the diverse components within the DOD can better coordinate acquisition, development, and support of DOD information systems. A current initiative is underway to transform this document into broader DOD applications that include C4ISR, Automated Identification Technology, and Weapons Systems.

- **Adopted Information Technology Standards (TAFIM VOL 7):** The TAFIM Volume 7, Adopted Information Technology Standards, should be used as guidance for standards in areas not addressed by the JTA.

- **DOD Human Computer Interface Style Guide (TAFIM VOL 8):** The DOD HCI Style Guide has been developed as a guideline document presenting recommendations for good interface design. The Style Guide is not intended to be strictly a compliance document; however, it does represent DOD policy concerning HCI design. The interface developer is expected to use the selected commercial GUI style guide, this Style Guide, and the appropriate domain-level style guide along with the input of human factors specialists to create the HCI.

2.5.5.4 The DII Common Operating Environment (COE) and the Shared Data Environment (SHADE)

The DII COE and SHADE provide detailed engineering specifications. The DII COE/SHADE define the operational environment for development and operation of Functional Applications including C2, mission support, and value-added services. They detail technical architecture guidelines, Applications Program Interfaces, integration standards, software tools, Human Computer Interface Specifications (style guide), data standards, and provide software executables and libraries. DII COE/SHADE are developed according to the TAFIM. See Appendix B.3, B.4. DII COE/SHADE compliance ensures that functional applications will be compatible with the supporting technical infrastructure and can interoperate with each other. The DII COE Integration and Run Time Specification (I&RTS) details the process for integrating functional applications into the DII COE. See Appendix B.3. DII COE/SHADE compliance ensures new DII applications and services can plug into the communications and computing infrastructure and can be made to interoperate.

2.5.5.5 Interoperability and Compatibility Certification

OSD and CJCS tasked DISA to certify that information systems and equipment meet the applicable standards and requirements for interoperability, compatibility, integration, and security. Independent testing and evaluation of DII elements for standards compliance and system interoperability assure that goal capabilities are verified from program inception. See Appendix C.8.

2.5.6 Summary

- Joint Vision 2010 provides the warfighter's vision, operational concepts, and requirements for leveraging technological opportunities to achieve new levels of effectiveness in joint warfighting. C4IFTW perfectly aligns with Joint Vision 2010. It provides the objectives and roadmap to focus unity of effort within the C4I community toward achieving Joint Vision 2010's vision, concepts, and requirements.

- The DOD ITM Strategic Plan has strategic objectives and performance criteria for the DII.

- The Service strategies complement C4IFTW. The Service strategies support normal and contingency warfighting capabilities in line with OSD and CJCS policy.

- The C4ISR Architecture Framework, the JTA, the DII COE/SHADE integration specifications, the DOD Goal Security Architecture, and compatibility and interoperability certification and testing

- The Component Program Plans are influenced by this guidance and reflected in the Components' POM submissions.

- Relevant guidance and key programs are summarized in the DII Master Plan.

(This Page Intentionally Left Blank)

SECTION 3

DII--SPECIFIC

3.1 Baseline Description

The present DII is largely an unintegrated collection of AISs. As such, it only partially meets the requirements of the DOD mission support and warfighting communities. Because it is unintegrated, there are redundancies and duplications that increase the cost of operations and thereby reduce the total resources focused on the DOD warfighting mission.

- The infrastructure is fragmented by multiple "stovepipe" information systems. This: (1) inhibits interoperability necessary to give commanders a unified picture of the battlespace; (2) reduces ability to provide links between the battlefield and the power projection support base; and (3) limits connection to the US industrial base.

- There is unnecessary redundancy and duplication of infrastructure elements. This results in waste and excessive cost that take dollars and manpower away from vital warfighting capabilities.

- The infrastructure is not planned, architected/engineered, acquired and operated from a DOD-wide perspective. This lack of DOD-wide perspective means that each mission area may develop its own capabilities instead of sharing resources, and the solutions may not be interoperable and integrated.

- Furthermore, existing capabilities are not adequate to meet current changes in mission, policy, and doctrine that are part of new warfighting and fiscal realities. For the warfighter, these realities include: the need to support Combined and Joint peacetime operations world-wide, to fight two simultaneous major regional conflicts anywhere, to adapt to flexible and changing force compositions, and to deploy a significant force rapidly and support that force from the CONUS and in-theater sustaining base.

3.1.1 Baseline Characterization by AIS Component

To support the planning and execution of DOD's Automated Information System (AIS) migration strategy, DISA developed a computer-based tool known as the Defense Integration Support Tool (DIST). The DIST facilitates the identification and selection of AIS migration for C2, combat support and intelligence systems; it can be used to obtain information characterizing the systems applications, data and infrastructure; and it can be used to conduct assessments, migration system selection, preparation of migration strategies and plans, as well as track the evolution of AIS. Additional information may be obtained at the following Internet sites: dist.disa.mil/submainpg/userssite.html and www.disa.mil:80/info/pao04m.html.

3.1.1.1 Data

DOD has few systems in operation today that use standard data elements. In response to this lack of standardization, the ASD(C3I) has made data standardization one of the top priorities for

the DOD. A DOD Data Administrator has been established as well as Functional and Component Data Administrators, to provide oversight and leadership. The web site, www-datadmn.itsi.disa.mil, contains additional information concerning DOD efforts for data standardization.

3.1.1.2 Application Software

DOD software applications frequently were developed as part of a dedicated information system, with computer hardware, system software, and communications. Within the Combat Support mission area, most of the application software is written in older programming languages that do not include modern software design concepts and documentation and have been changed significantly through the years without appropriate configuration management processes. In the C2 and Intelligence mission areas, application software tends to be developed in more modern languages and to be better documented. Within the C2 mission area, the conventional operations application software is being migrated to the GCCS, which will be an open, distributed information system that relies on a COE of support application software and system software and hardware. The intelligence community has similar migration plans. The Department of Defense Intelligence Information System (DoDIIS) will provide a client/server environment with open, standard system software and application software for a large portion of the intelligence community. In addition, some DOD communities have begun to standardize EDI formats and messaging services for information exchange with other government agencies, allies, industry, and academia. At the desktop in the DOD, application software ranges from terminal emulation for mission data access to COTS office automation applications. Virtually no cross-mission integration has occurred at the desktop.

3.1.1.3 Hardware

Local processing environments for both mission facilities, such as command centers, and for the installation level, including office automation, tailored, and field applications, are heterogeneous and have relied almost exclusively on non-open systems. Migration to open system and client/server implementations currently are starting for some applications. At data processing installations, some homogeneity in hardware has been achieved through Defense Megacenter consolidations. However, heterogeneous operating environments generally do not conform to open systems standards and rely on custom software, resulting in difficult data interchange, limited software reuse, high license costs, and conflicting and duplicated data with unique structures and definitions within and across DOD mission areas.

3.1.1.4 Communications

Tactical systems are rarely integrated with other segments of the DII, limiting the effectiveness of wartime operations. Uniform standards are not being applied in present implementations, causing interconnection problems. Several efforts are underway to provide enhanced strategic-tactical communications interfaces and integrated management for C/JTFs. The Sustaining Base includes data networks that may be isolated from the rest of the infrastructure and switched systems that vary in age and technology. Long-haul communications programs are integrating data, voice, imagery, and video services across organizations and functions to meet increasing integration requirements. However, separate systems still exist. Dial-up circuits for

communications are still prevalent within the DOD and with external organizations such as vendors and other Federal Agencies. The DOD increasingly is using the Internet to access external sources and exchange electronic mail with external organizations. Security concerns have limited the availability of this resource for many DOD organizations. The DOD is addressing the issue by participating in appropriate fora to develop security mechanisms such as firewalls.

3.2 Roles and Responsibilities

Figure 3.2-1 shows some DII elements, along with organizational responsibilities. These responsibilities, taken together, ensure that every aspect of the DII will be addressed.

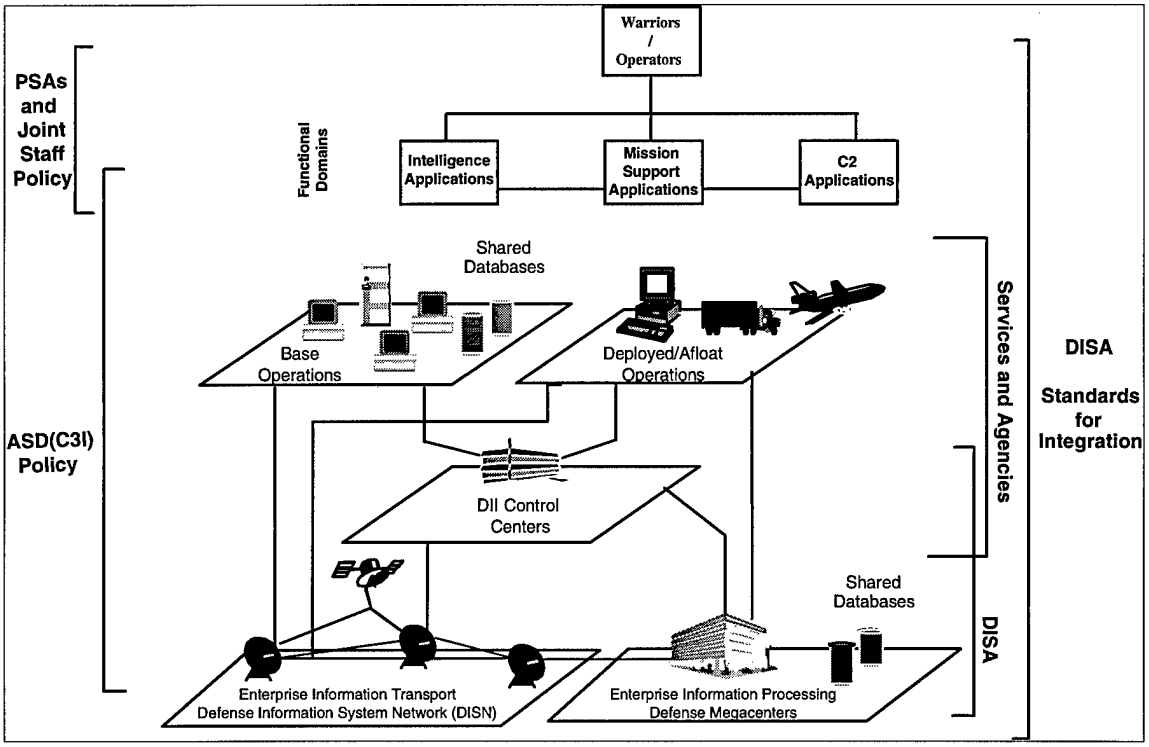


Figure 3.2-1. DII Roles and Responsibilities

Roles and responsibilities are discussed in the Appendices for each DII Element. Overall, DII responsibilities are as follows:

- The OSD PSAs and the Joint Staff establish policy and plan for mission applications, including data requirements for C2, intelligence, surveillance, reconnaissance, and combat support functional areas.

- The Joint Staff validates Joint requirements for C4I systems. The J6, helped by DISA, certifies interoperability aspects of Mission Need Statements and Joint Operational Requirements documents for C4I systems.

- The Military Services and Defense Agencies design, acquire, and develop mission applications.

- The Military Services and Defense Agencies install and operate the sustaining base and the C/JTF deployed/afloat elements of the DII.

- DISA installs the enterprise-level DII Elements (e.g., long haul DISN and the Defense Megacenters) and shares operations and maintenance responsibilities with the Military Services and Defense Agencies.

- DISA and the Military Services and Defense Agencies share in the installation, and operation of the DII Control Centers that manage the DII.

- ASD(C3I) sets policy for the DII, including the sustaining base, deployed, and DOD-wide elements.

- DISA, the OSD PSAs, and the CINCS, Military Services, and Defense Agencies (C/S/As) collaboratively select the standards for integrating the DII elements.

- DISA, in coordination with the C/S/As, develops and maintains the DII standards-based architecture.

- The Joint Staff provides operational direction for the DII.

- Information Security is a shared responsibility. ASD(C3I) sets policy. DISA and NSA in collaboration with C/S/As, identify threats and requirements. The Joint Staff validates requirements. All DOD Components implement the policy.

- The Military Communications Electronics Board (MCEB) is the resolution authority for the Military Services, Unified Combatant Commands, and Defense Agencies to help in the resolution of issues related to interoperability and standards. Unresolved interoperability issues will be worked by the MCEB Interoperability Improvement Panel. Unresolved standards issues will be worked by the MCEB Standards Coordinating Committee. If issues cannot be resolved by these panels, they will be forwarded through the MCEB Secretariat for action at the coordinator level or final resolution by the MCEB principals. See section C.1.2.2.

Key councils supporting the DII include:

- Defense Information Infrastructure Resource and Operations Council (DIIROC). The 14 May 1997 memo signed by the ASD(C3I) tasked DISA to establish a DIIROC which is to act as a board of directors for the DII. Composed of the senior C4 leaders from the Services, Joint Staff, DISA, and NSA, this council is charged to establish goals for the DII's continued evolution, to raise issues affecting the warfighters and service providers, and to resolve issues for the benefit of the DOD.

- DOD Architecture Coordination Council (ACC). The ACC was formed in January 1997 to establish comprehensive architectural guidance for the Department and to determine how the DOD should "rationalize and synchronize" ongoing architecture work. The Council is chaired by the USD(A&T), ASD(C3I), and the Director, Joint Staff.

- Defense Management Council. This council emerged from the November 1997 Defense Reform Initiative. Chaired by the Deputy Secretary of Defense, it will be responsible for recommending to the Secretary of Defense major DOD reforms still needed, ensuring the implementation of those already identified, and continuing the oversight of the Defense Agencies.

3.3 Requirements and Objective Environment

The DII is evolving to an objective environment that is derived from strategic, operational, technology, enterprise, and fiscal influences. The appendices describe the requirements and objective environment of each of the major DII elements in more detail. At the beginning of each appendix is a brief overview of the DII elements in the appendix.

3.3.1 Requirements

The DII is to support national military policy and the current joint doctrine based on C/JTFs formed with scaleable force mixes to respond to a wide spectrum of potential conflicts. The National Military Strategy envisions power projection by highly flexible, rapid-response, tailored force packages under C/JTF command. To support this strategy, the C4IFTW concept guides all the Military Services toward a global C4I system that creates a single view of joint military C4I. This view is of a widely distributed, user-driven infrastructure to which the warrior "plugs in." The DII must respond quickly to new joint, coalition, and organizational relationships created on demand and to the C4IFTW vision of a fused, real-time, true representation of a three-dimensional digital battlespace with the ability to coordinate in all directions. The changing operational context in which the DII must operate to support the warfighter includes:

- Deployed, tailored force packages under C/JTF command
- Regional orientation
- Wider range of missions
- Uncertain, unknown threats
- Ad hoc coalitions or unilateral operations
- Adaptive planning and strategic agility
- Smaller total force, reduced forward presence
- Rapid response capability
- Variable foreign infrastructure sophistication; uncertain access
- Increased use of precision targeting

The C4IFTW initiative sets forth a concept for global C4I that: (1) will allow any warrior to perform any mission, any time, any place; (2) is responsive, reliable, and secure; and (3) is affordable. Based on the C4IFTW concept, the DII must provide and support:

- Flexible, modular C4I packages
- Timely, consistent information exchange
- Transportable, rugged, and wearable resources
- Real-time decision making
- Full interoperability
- Adaptive safeguards and security with assured service
- Horizontal and vertical C2
- Common operating environment
- Global C4I resource management and control
- Fully integrated information (fusion)
- Seamless operations
- Smart push (over-the-air updating)
- Warrior pull-on-demand
- Reachback and split base operations
- Bandwidth on demand

To meet these requirements, DII users must be able to work collaboratively over long distances and across time. DII users must be able to access information and resources transparently when needed without knowing their location and automatically scan for required information and special events in information stores within and outside of the DOD. DII users must be able to access their personal information environment transparently from anywhere and reach all other users on interconnected networks via voice, data, imagery, video, or some combination of these media. DII users must be able to access information, resources, and capabilities while providing their activities the security required to protect national interests. DII users must be able to integrate data and applications across functions (e.g., C2 and Intelligence). The DII must operate in a distributed, heterogeneous information services environment and must continue to evolve to support new missions and provide new capabilities. Information must be able to be stored in many ways and at many levels of detail. The DII must recognize the heterogeneity of systems that exist and accommodate the integration of these components as well as the integration of new technology.

3.3.2 Objective Environment

To support the operational requirements described above, the DII must be:

- *Interoperable*–allowing connectivity and interchange of information among information resources at the network, application, presentation, and data levels as required without special connections, procedures, or other intermediate translation and gateway devices
- *Transparent*–providing the user with a virtual information services environment such that the user does not need to know where the applications and data reside
- *Scaleable*–supporting information system environments from large, fixed facilities and networks to hand-held and wearable devices in the battlefield
- *Responsive*–guaranteeing assured services, quickly available, when and where needed worldwide under varying degrees of stress

- *Secure*–implementing multiple security policies and assuring required information system and communications security and availability
- *Easy to use*–providing intuitive interfaces tailored to the user' s preferences
- *Flexible and maintainable*–allowing quick migration and integration of new applications and technology (e.g., through the use of standards-based and vendor-independent approaches)
- *Reliable*–supporting alternative resource and service access or graceful degradation
- *Affordable*–providing the best value for required services (and only required services) in the most efficient way available consistent with mission needs
- *Evolvable*–including special methods, metrics, tools, and environments that use the DII to evolve to new missions and capabilities
- *Survivable*–Ensuring that essential information is available to meet mission requirements under varying conditions of stress.

The operational DII will be constantly changing, and consequently will need engineering methods, tools, and metrics to plan, evaluate, and support its evolution. A distributed, network-accessible database approach will be needed to keep an up-to-date view of the evolving DII, so that planning can reflect reality. Performance assessment data for computer systems and communications networks will be essential to planning this evolution and evaluating options. Integrated, distributed development environments addressing networks, systems, applications, data, and security and focused on development of distributed systems will be necessary and will require software reuse libraries, data dictionaries, and workflow management tools.

3.4 Strategy

The DII strategy addresses how DOD Component initiatives come together to achieve the C4IFTW vision. The strategy has six strategic thrusts:

- Validate Joint requirements and oversee acquisition
- Establish innovative vehicles to acquire IT
- Provide a common technical approach for achieving compatibility, interoperability, integration and security of the DII
- Plan collaboratively
- Assess programs jointly
- Coordinate operational direction and control exercised by the DII Operations Control Complex (DOCC)

3.4.1 Validate Joint Requirements and Oversee Acquisition

The SECDEF and the CJCS are establishing a powerful mechanism for ensuring that warfighter requirements will drive the evolution of the DII. Top-level directives and instructions for information systems are in place to ensure that DII elements developed in parallel by the various DOD Components will have compatibility, interoperability, and information security built in and validated from program inception.

Evolution of the DII will be driven by Warfighter requirements.

Mission needs result from ongoing assessments of current and projected capability. The C/S/A develop Mission Needs Statements (MNS), Joint Operational Requirements Documents (JORDs) that identify specific functional needs. If the potential solution could result in a new AIS, the appropriate OSD PSA and the Joint Requirements Oversight Council (JROC) review the MNS or JORD. They determine its validity, establish Joint potential, and confirm that the requirements defined in DOD Directive 8000.1 are met. C4I system requirements are validated according to OSD and CJCS established processes There is no MNS or JORD for the DII since it is not a single program. However, many DII initiatives (e.g., DISN, DMS) are implementing Joint validated requirements.

New technologies (e.g., Direct Broadcast Satellite) can provide capabilities not previously envisioned by the warfighter. The JROC initiated C4ISR Joint Battle Center will provide a process for continuous technology insertion and the capability to affect interoperability during the early stages of concept exploration and system development. Lessons learned guide the development of mission needs and joint operational requirements for promising new concepts and technologies. (see Paragraph C.6)

After the JROC and the cognizant OSD PSA validate a mission need, the ASD(C3I) determines whether the new program will be overseen by the Major Automated Information System Review Council (MAISRC) or by the lead DOD Component.

The MAISRC oversees Major Automated Information System (MAIS) acquisition programs that are: (1) designated by ASD(C3I) as a MAIS, or (2) estimated to require program costs in any single year of more than $30M in FY1996 constant dollars, total program costs more than $120M in FY96 constant dollars, or a total life-cycle costs more than $360M in FY96 constant dollars. The preponderance of acquisitions, are overseen by the responsible Military Service or Defense Agency. All oversight is done according to DOD Directive 5000.1, and DOD Regulation 5000.2-R.

3.4.2 Establish Innovative Vehicles to Acquire Information Technology

The DOD Components are implementing DII capabilities in parallel. The capabilities can be viewed as DII products and services. The following vehicles provide DOD IT managers with quick access to IT products and services at competitive prices.

- **The Defense Enterprise Integration Services Contract (DEIS II)** provides contractual vehicles for all DOD Components to obtain contractor services for: functional requirements definition, identification, validation, migration system selection, baselining, benchmarking, business process reengineering, prototyping, development, deployment, operations and maintenance of these systems. Functional area applications developed under this contract will be deployed, and sustained in the DII COE using shared data, where feasible, and utilizing common communications, messaging, security, processing solutions in compliance with DOD architectures, standards, and guidelines. Services provided under DEIS II will be obtained through individual task orders providing specific details of the technical requirements. Several teams of vendors are available, allowing

DOD managers to get the best value for their IT dollars.

- **Products and Services.** DISA provides many DII products and services to the C/S/As, and non-DOD activities as well. DISA can provide information technology solutions for mission critical applications in a secure environment. The core DII services are: telecommunications, computing, and integrated services. DISA provides some processing and telecommunications services on a fixed price, reimbursable basis, while others are provided by DWCF activities. In April 1997, DISA developed the DISA Products and Services Information Catalog that provides generic descriptions of product and service lines as well as points of contact. The catalog will evolve to include additional descriptive details and links to existing major DII elements and on line ordering process as they become available. The catalog is on the Internet (www.disa.mil/prodserv/pscathp.html). DISA is implementing a COTS system called MONIES for provisioning that will replace existing systems within a year. MONIES will be coupled with the DISA Products and Services Information Catalog and will be the primary means for customers to order all DISA products and services.

- **Enterprise Licensing and Electronic Shopping.** DISA has established basic ordering agreements for quick delivery of DII COE and SHADE software and hardware at prices significantly below the Government Services Agency (GSA) Schedule. These agreements are administered for DISA by Fleet Industrial Supply Center detachment in Philadelphia and Naval Transportation Service Center (NTSC), Jacksonville. DOD IT buyers have a vehicle to buy products from about 30 vendors. DII COE hardware products can be purchased through electronic shopping kiosks located in the Pentagon, Hanscom Air Force Base (AFB) and other locations. Products are delivered to the buyer from 3 to 30 days after receipt of the buyers purchase request. Additionally, the DOD Integrated Computer-Aided Software Engineering (I-CASE) contract offers substantial savings on enterprise software licenses. The I-CASE Program Management Office is within the Headquarters Standard Systems Group at Maxwell Air Force Base. The I-CASE contract was recently revamped and products on the revised contract support the DII COE.

The following are some other support services contracts that contribute to the development of the DII.

- **DISN Support Services Global (DSS-G).** Support services to assist in fulfilling DISA's mission of providing cost effective, responsive, worldwide information services as described in the DISN Program Strategy. The support services may be used worldwide to support classified and unclassified voice, data, imagery, video, and transmission components of the DISN.

- **INFOSEC Technical Services Contract (ITSC).** Engineering services and technical support to produce unified, fully integrated systems security solutions for the DOD.

- **JIEO Systems Engineering (JSE) Contract.** Foundational engineering work to include telecommunications, computer systems engineering, standards, application software development, and general engineering.

- **DII Integration Contract (DII IC).** Provides intense level of integration support for globally fielded DISA programs. It will integrate, segment, test, and field mission applications developed under other contracts. It also will define, build, and field SOE and SHADE as well as common support applications.

- **DII COE Contract:** Develops the core building blocks of the DII COE. Requires highest level of integration intensity. Develops infrastructure services, operating systems, tools, multi-platform support, and application programming interfaces for COE.

3.4.3 Provide a Common Technical Approach for Achieving Compatibility, Interoperability, Integration, and Information Security of the DII

Compatibility, interoperability, integration, and information security are key goals that must be satisfactorily addressed for all acquisition programs. These goals will be specified and validated during the requirements generation process. Satisfaction of these requirements will be addressed throughout the acquisition life-cycle for all acquisition programs. Interoperability of C4I systems will meet DOD Directive 4630.5, DOD Instruction 4630.8, and CJCS Instruction 6212.01A.

Military Service and Defense Agency implementers need technical architectures, standards, tools, and processes to guide them through thousands of detailed engineering decisions and tradeoffs that can enhance or inhibit system compatibility, interoperability, and security among DII elements.

Components will implement and validate systems in accordance with the C4ISR Architecture Framework and the JTA. The GCCS and GCSS initiatives help DOD Components integrate capabilities into the DII COE and SHADE. The DOD Components will use business process reengineering to examine and evolve combat and combat support processes to further improve mission effectiveness and reduce costs.

Information Technology program managers have been directed to use the set of "building codes" described in the JTA and underlay the DII COE and SHADE, to construct systems that are compatible and interoperable from program inception. See Paragraph 2.5.5 for an explanation on the relationship between DOD technical guidance documents.

3.4.4 Plan Collaboratively

The ASD(C3I) needed a plan to ensure that the right resources are programmed to do the right things, at the right time, by the right organizations. ASD(C3I) tasked all DOD components to work together to build the DII Master Plan. The DII Master Plan Working Group has worked together to produce the plan and continually improve it. Working group members are

Management oversight will be provided by existing bodies for acquisition oversight, collaborative planning, Joint assessment, and operational direction.

listed inside the front cover of this document.

The TAB-G exhibit of the POM is intended to capture the entirety of the DOD's programmed consumption of computer and communications infrastructure and functional areas AISs. ASD(C3I) worked with the Under Secretary of Defense (USD) (Comptroller) and Military Service and Defense Agency representatives worked together to develop clearer guidance for POM preparation. The TAB-G instructions developed by the team will make reporting more uniform for C&CI, and the functional area AISs within the Military Service and Defense Agency POMs and across the DOD. The discussion of DII Elements in the DII Master Plan is aligned with the categories defined in TAB-G to make cross-walking easier.

Collaborative planning is also going on at the program level. DMS, other DII initiatives are being reviewed by the MAISRC. GCCS and GCSS are working hand-in-hand with the C/S/As and PSAs to develop implementation plans and schedules for integrating functional applications into the DII COE and SHADE. Program plans, implementation plans, technical architectures, interoperability and standards are being worked by many working groups. The DISN Program Office is in the process of establishing a DISN Integrated Process Team with ASD(C3I).

3.4.5 Assess Programs Jointly

The Joint Warfighting Capability Assessment (JWCA) initiative (CJCSI 3137.01) operates within the Program Planning and Budgeting System (PPBS). The JWCA C2 team identifies critical C4I issues, priorities, and performance goals to the JROC to help the Chairman in developing the Chairman's Program Recommendations (CPR), and the Chairman's Program Assessment (CPA). The CJCS draws from the JWCA process and the advice of the JROC to fulfill his statutory responsibility to provide advice to the SECDEF regarding program recommendations and budget proposals. The CPR is delivered early in the PPBS cycle providing input to the programming and budgeting process before completion of the DPG. The CPR articulates issues the CJCS deems critical for the SECDEF to consider when identifying priorities and performance goals in the DPG.

The DPG initiates the PPBS cycle. It issues SECDEF guidance for development of the Components' POM. The DPG includes major planning issues and decisions, policy, strategic elements, the SECDEF program planning objectives, the Defense Planning Estimate, and illustrative planning.

The CJCS, helped by the JROC and JWCA process, reviews the Military Service and Defense Agency POMs and the preliminary program decisions made regarding the Defense Program. The CPA, delivered near the end of the PPBS review cycle provides the CJCS's assessment of the adequacy of the Military Service and Defense Agency POMs, as defined in the most recent programming cycle. It also includes an evaluation of the extent to which the POMs conform with the priorities established in strategic plans and the CINCs' requirements.

Through the CPR and CPA the JROC and JWCA C2 team exercise considerable influence in keeping DOD Component programs focused on warfighting needs and aligned with the goal envisioned by both the Joint Planning Document (Volume 3) and C4IFTW.

3.4.6 Coordinate Operational Direction and Control Exercised by the DII Operations Control Complex (DOCC)

A DISA Circular 310-50-5 with the same title as this subparagraph (on the Internet at: www.disa.mil/d3/drftpubs/310505/cover.html) is being coordinated with the C/S/As. The circular establishes the policy for exercising operational direction and control over the DII and prescribes the operational principles and functions of the DOCC. A second document, "Joint Defense Information Infrastructure Control System Concept of Operations (JDIICS CONOPS)," discusses a Joint management concept that will provide the positive control and protection necessary to achieve the required confidence in the DII. A copy of the JDIICS CONOPS can be obtained by contacting Lt Lisa Rawson at rawsonl@ncr.disa.mil or Mr. Lou Morgan at morganl@ncr.disa.mil.

3.5 Near-Term Programs and Initiatives

Major near-term initiatives are identified in Paragraph 3.6, below. Near-term programs and other initiatives are also identified in the appendices for each major DII element.

3.6 Schedule

Figures 3.6-1 through 3.6-4 present some of the major DII milestones through FY99. The schedules are intended to help identify key decision opportunities and discontinuities in synchronizing DII efforts across DOD. See the appropriate appendix for details.

ID	Communications & Computer Infrastructure	1997				1998				1999				2000			
		Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4
1	*DISN*																
2	FOC CONUS Trans svcs					•											
3	FOC CONUS B/WIDTH man						•										
4	FOC VIDEO SVC - Global						•										
5	IOC DISN Teleport												•				
6	IOC STEP												•				
7	IOC GBS						•										
8	IOC MSS								•								
9	*Megacenters*																
10	TBD																
11	*Control Centers*																
12	Policy Definition						•										
13	Customer Access System						•										
14	ROSC INT into GOSC				•												
15	*Base, Deployed, Afloat Infrastructure*																
16	TBD																

Figure 3.6-1. Communications and Computer Infrastructure Schedule

ID	Common Applications	1997				1998				1999				2000			
		Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4
1	*DMS*																
2	Release DMS 2.0 Development						•										
3	INFOSEC Detect Tools									•							
4	DMS 1.1 Testing						•										
5	DMS Service Schools					•											
6	AUTODIN Shutdown													•			
7	*EC*																
8	DMC NEPS Cutover		•														
9	*DII COE*																
10	Release COE					•											
11	*SHADE*																
12	Common Data Access					•											
13	*IDM*																
14	GBS IOC													•			
15	Connectivity											•					
16	Services					•											

Figure 3.6-2. Common Applications Schedule

ID	Foundation	1997				1998				1999				2000			
		Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4
1	*Policy*			•													
2	DODD 4630.5 & DODD 4630.8			•													
3	Revise DODD 8000.1								•								
4	*Requirements*																
5	Functional Requirements Documents	•	•	•	•												
6	Develop AMETLS					•											
7	Develop UJTL/JMETL	•	•	•	•												
8	*M&S*																
9	Delivery of Netmaker 3.0					•											
10	JSIMS POC												•				
11	*Joint Spectrum Management*																
12	JSC Modernization Program	•	•	•	•	•	•	•									
13	Spectrum XI IOC	•	•	•	•	•	•	•	•	•							

Figure 3.6-3. Foundation: Program and Technical Activities Schedule

ID	Functional Area Applications	1997				1998				1999				2000			
		Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4
1	*C2*																
2	GCCS SOR (3/96)																
3	GCCS V3.0			•	•	•	•	•	•								
4	GCCS (T)		•														
5	GCSS COE	•	•														
6	GCSS Cluster 1				•	•	•	•	•								
7	GCSS Cluster 2	•	•	•	•	•	•	•									
8	GCSS Cluster 3				•	•	•	•									
9	GCSS Cluster 4		•	•	•	•	•	•	•								
10	GCSS Cluster 5		•	•	•	•	•	•									
11	*Procurement*																
12	*LCM Program*																
13	Release 1 Deploy					•											
14	Release 2 Deploy						•										
15	Release 3 Deploy															•	
16	*Nuclear Chemical Biological*																
17	NUMIS- FOC			•													
18	NUCWAR Replace NUCOM						•										
19	OSMAPS SW/HW Upgrades							•									
20	NUMIS_M DII COE Compliant								•								
21	*Health*																
22	Implement TRICAR	•	•	•													
23	Theater Telemedicine	•	•	•	•	•	•	•	•								
24	DBSS					•	•	•	•								
25	TRAC 2ES/PARRTS	•	•	•	•	•	•	•	•	•	•	•	•				
26	*Intelligence Applications*																
27	Install DoDIIS COE Infrastructure				•	•	•	•									
28	*Combat Support*																
29	Implement DII Support Capabilities							•									

Figure 3.6-4. Functional Area Applications Schedule

3.7 Resources

The following information is drawn from the TAB-G annex to the Services' and Defense Agencies" FY 99-2003 POM. The TAB-G is the closest thing we have to a "roll-up" of the portfolio of programs contributing to the DII, along with their associated resources. The TAB-G of the POM has the following characteristics:

- TAB-G reports through Budget Year (BY) 2+4 (BY2+3 in second year of biennial submissions).
- TAB-G reports detail on initiatives and automated information systems (AISs) at a threshold of greater than $2M in one FY or greater than $25M over the life cycle.
- TAB-G reports C&CI resources for Communications and Computing Infrastructure (C&CI), functional area AISs, and Related Technical Activities (RTA). IT Budget exhibits do not normally break out the infrastructure resources in as much detail as does TAB G.
- TAB-G reports all C2 systems resources except those used for weapons systems training, simulation, diagnostics, testing, maintenance, calibration, or highly sensitive, special access AISs.
- Some of the C2 system resources reported in TAB G are exempt from reporting in the IT Budget.
- TAB-G reports non-sensitive intelligence systems, which may be excluded from the President's budget submission.

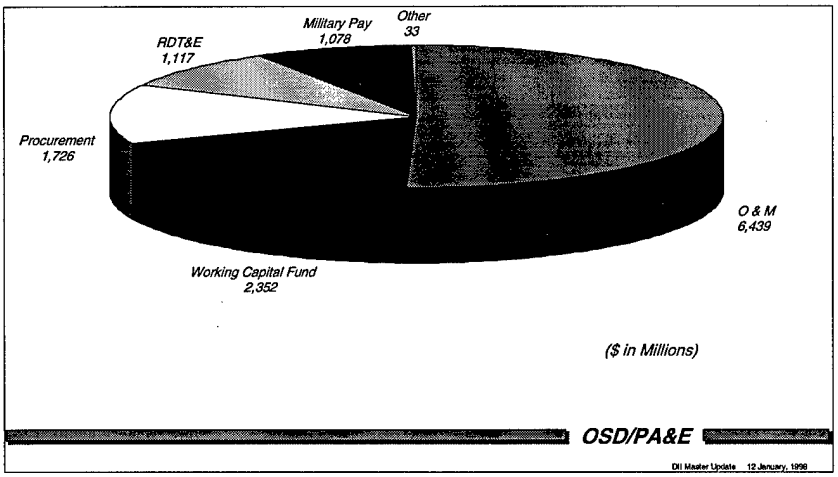


Figure 3.7-1. FY98 IT Budget by Appropriation

Figure 3.7-1 illustrates the TAB-G broken out by appropriation. Information technology (IT) is a strategic resource without which key DOD initiatives cannot succeed. Investments in IT enable DOD Components to streamline, redesign work processes, and improve service delivery. The bulk of the DOD IT budget is financed through the Operations and Maintenance (O&M)

fund, and the DWCF. O&M and DWCF account for just about 70% of the DOD IT budget.

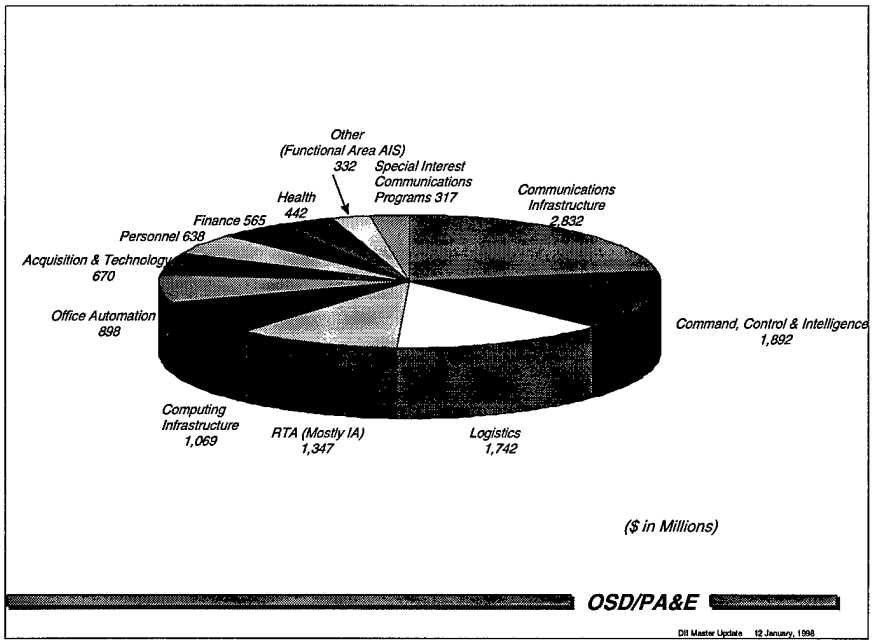


Figure 3.7-2. FY98 IT Budget by Function

Figure 3.7-2 shows the IT budget broken out into the major categories identified in the DII Master Plan and the TAB-G. About half of the resources are directly attributable to C&CI and RTA (primarily Information Assurance which can be considered part of the infrastructure). The other half of the resources are associated with the development or operation of functional area applications or AISs. The resources associated with AIS programs include significant funding for application-specific hardware, particularly in the C2 and logistics areas.

	FY98	FY99
Army	2,407	2,417
Navy/USMC	2,867	2,970
Air Force	3,023	3,043
Defense Agencies	4,447	4,511
Total	12,744	12,941

$197 Million Increase(FY98-FY99)

($ in Millions)

OSD/PA&E

Figure 3.7-3. Changes from FY98 to FY99

Figure 3.7-3 shows the information technology budget by DOD Component. This information

was also drawn from TAB G for FY99-03, and the funding shown is somewhat larger than that provided with the President's Budget. The funding is also greater than the funding shown in last year's DII Master Plan because more C2 systems have been captured in TAB G than in previous years. FY 1998 funding shown in the FY99-03 TAB G is $12.744 billion; for FY 1999 it is $12.941 billion.. The Defense Agencies account for about a third of this amount, reflecting their responsibility for developing, fielding, and operating many of DOD's functional area AISs, particularly joint-Service migration systems.

3.8 Interdependencies

The NII is a Federal-level initiative, in concert with industry, and state and local Governments, to develop a national high-speed information processing and transfer network. Evolution of the NII includes national telecommunications policy reform to encourage growth of the information industry. The NII is by definition, national in scope. The DII uses the NII in combination with U.S./Allied military and commercial overseas information infrastructure to meet the global information needs of the DOD.

The DII uses the NII in combination with U.S./Allied military and commercial overseas information infrastructure to meet the global information needs of the DOD.

The DII provides interfaces for DOD customers to other sources in the NII and to U.S. Allies. The DII also can provide information services to selected non-DOD customers. For example, service could be extended globally for NII customers through existing DII capabilities. Also, strategic cooperation between the DII and the NII organizations will foster development of: dual-use technologies, technology transfer, and information technology standards. Side benefits include: Defense conversion to reduce the cost of providing information services, and increasing U.S. global competitiveness in information technologies. NII and DII linkages are discussed in Appendix B.

3.9 Performance Measures

Performance measures must be selected and engineered to achieve management purposes. The following paragraphs develop the framework and outline an initial set of performance initiatives to accomplish DOD ITM Strategic Plan objectives.

3.9.1 IT Performance Measurement

The Clinger-Cohen Act, Section 5123, states: "...the head of an executive agency shall – (1) establish goals for improving the efficiency and effectiveness of agency operations...(3) ensure that performance measures are prescribed for information technology used by or to be acquired for, the executive agency and that the performance measurements measure how well the information technology supports the programs of the executive agency. The Act also refers to the need to manage IT as an investment; that IT provide mission benefit and enhancements; that progress be measured; and that the outcome/results of our IT investments be evaluated.

Performance measurement is a mechanism for helping managers improve mission performance. Quantifiable goals challenge organizations and individuals to make improvements in how they accomplish their tasks toward achieving their missions. Measuring the progress of the tasks can focus attention on what is most important to the mission, thus measures can be used to drive changes in culture, processes, and IT. Figure 3.9.1-1 is a generic performance measurement "process map". This map was derived from the work of the NPR Benchmarking Consortium Study, (draft) January 29, 1997.

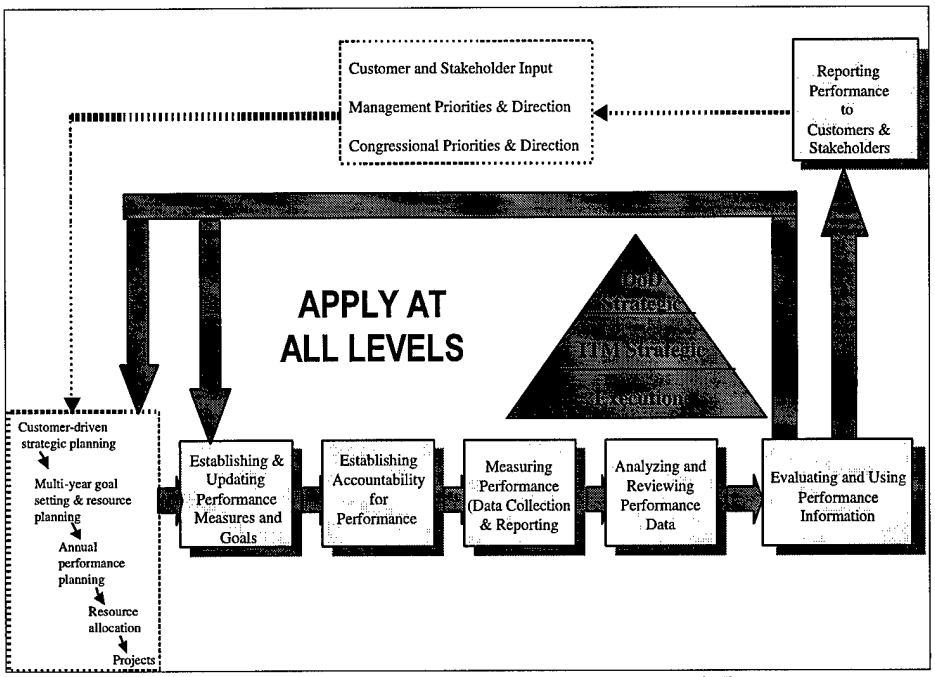


Figure 3.9.1-1. Performance Measurement Process Map

The measurement process can support the key management activities of any agency by gauging the performance of or progress toward customer-driven strategic planning; long-range visioning and goal setting; annual performance planning; resource allocation; and implementation projects. Managers who know the progress or performance of any given program or process, are in a better position to perceive risk factors, project likelihood of success and thus make sounder decisions.

The process is iterated to evolve the organization to higher levels of performance. Equally important, a measurement infrastructure must be put in place. This consists of training, databases, and tools to assist organizations to collect, process, maintain, and assess measurement information. A more mature measurement management process is one in which the basic process is applied at the DOD IT strategic and implementation levels and measures are integrated across levels to ensure that they are consistent and drive the Department towards its leadership's vision for the future.

3.9.2 Strategic Measures Context.

DOD strategic plans containing high level goals and objectives cascade down to link to strategic plans of the functional activities. Performance measures at these levels also cascade down as far as execution levels to gauge progress towards the strategic goals and objectives of the various levels of plans. At the strategic level, performance measures gauge the IT contribution to the defense mission. At the functional level, performance measures would indicate contribution to the functional goals and objectives which are in turn linked to the DOD mission. At the execution level, individual programs report progress using their IT Performance baselines for cost, performance, and schedule. The data collected from measures at the lower levels are summarized so that CIOs and others leaders can gauge, from a strategic perspective, how well the Department is meeting its IT and mission challenges. (For example, the average time to field a new system in DOD can be aggregated from Component data.)

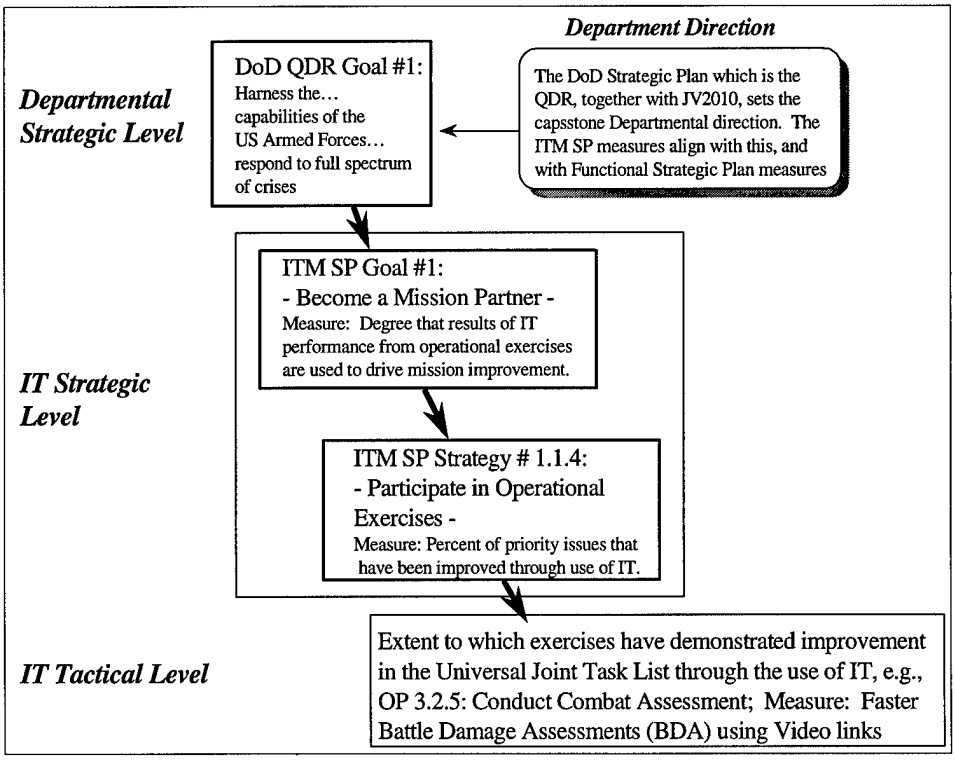


Figure 3.9.2-1. Flow of Measures from Strategic to Tactical Levels

The ITM Strategic Plan is linked to the vision and goals of the Department. The Plan is aligned with JV2010, the DOD Strategic Plan/QDR, and functional strategic plans. Figure 3.9.2-1 shows the flow of measures from the DOD top level, through the ITM Strategic Plan, to a very specific and critical warfighting mission. This typical thread will be repeated hundreds of times resulting in measurable achievement of Information Superiority and other top DOD goals.

Developing and using ITM strategic measures is evolutionary and incremental. Measures will be deployed across DOD systematically to allow organizations to learn and build their measurement systems, skills, and competencies. Measures can help organizations use customer surveys to

gauge customer satisfaction. Near-term indicators show survey instruments have been developed and are beginning to be used. In the mid-term, measures will indicate the robustness and depth of the survey process. Long-term measures will show managers how IT organizations use the surveys to improve customer services and responsiveness. Figure 3.9.2-2 shows the phased evolutionary approach.

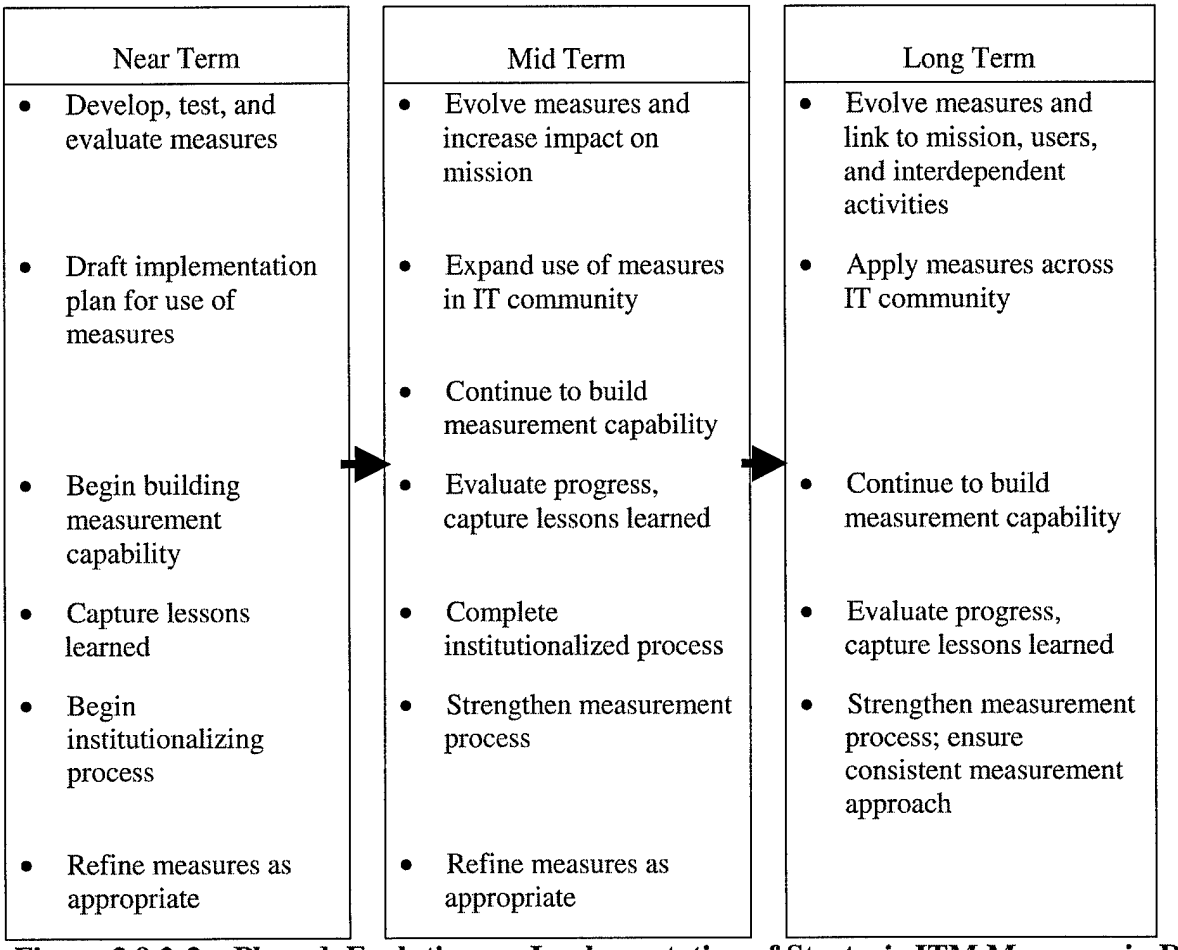


Figure 3.9.2-2. Phased, Evolutionary Implementation of Strategic ITM Measures in DOD

Each organization must establish its own tailored measures program to assess and improve its performance and provide summary information to the IT strategic measurement process so higher levels can gauge overall performance. These objectives are fully compatible because the Department is developing a consistent and integrated ITM program "top-to-bottom" -- the IT goals and measures of command and field activities will link back to Component IT goals and measures, and these in turn will be aligned with DOD ITM strategic goals and measures. Measurement against common IT goals will be accomplished at different levels of detail to support the decisions that must be made at each organizational level.

Due to the variety of IT activities at different stages of maturity in their use of measures, it is necessary to build-in flexibility in the DOD measurement process. Today, some organizations may be extensively applying customer surveys. Other organizations may be emphasizing the use

of Baldrige self-assessments or the Software Engineering Institute's (SEI) capability maturity model. Over time, there will be a convergence to a more uniform measurement approach.

3.9.3 Implementation Management – Two Pilot Projects

Achieving the long-term commitment to ITM measures requires coordinated planning and implementation. Thus the Department has embarked concurrently on two high level pilot performance measurement pilots: a core set of measures for the goals in the DOD ITM Strategic Plan; and the CIO Executive Level Performance Measures for major improvements in the ITM processes of selection, control, and evaluation. The CIOs, working together, will harmonize these capstone pilots and assess progress toward institutionalizing the use of ITM measures across the Department. Figure 3.9.3-1 shows the implementation management process.

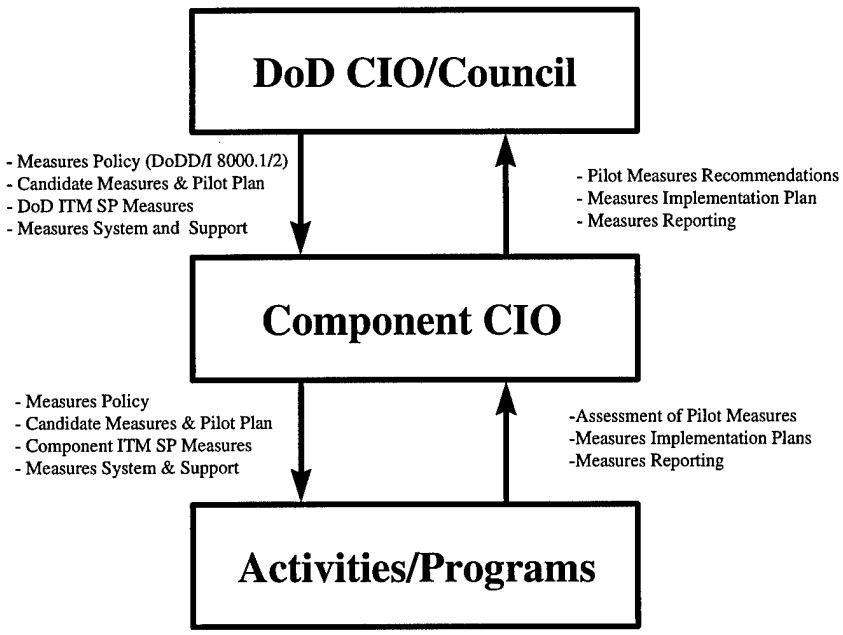


Figure 3.9.3-1. Measures Implementation Management

3.9.3.1 ITM Strategic Plan Measures Pilot

This pilot supports an incremental approach to strategic performance measurement, focusing on Goals 1 and 2 of the ITM Strategic Plan. Specifically, it implements the near term phase described in the "Strategic Measures Context" section above. An initial core set of strategic measures will be piloted before they are institutionalized to validate that they are useful and practical. They will be expanded to address more aspects of ITM as they are validated. Based on a high level implementation plan, volunteer organizations will develop implementation plans and begin component level pilots in early 1998. These organizations will report the results of their pilots to the DOD CIO. They will share successes, obstacles, and recommended refinements to the performance measures.

The pilot will provide a basis for recommendations on how to institutionalize the process and the measures. From the pilot results, the DOD CIO will establish strategic goal performance measures in the next update of the ITM Strategic Plan. Components will inherit the goals and measures in the DOD ITM Strategic Plan, and in turn, include them in their ITM Strategic Plans and issue component level guidance and policy. This will ensure consistency leading to greater jointness, a common infrastructure, and a system of systems architecture. Components may extend and amplify these measures to meet their specific missions and leverage their core competencies.

The Department will issue guidance and policy for measures. Guidance will flow down into subordinate activities and implemented through IT initiatives, programs, investment portfolios, and projects. This will ensure uniform, timely reporting of measurement information at each level. Actual performance measures will be reported to Component CIOs for evaluation. This information will be aggregated and summarized up to the DOD CIO and CIO Council, and other high level functional managers to help leadership evaluate Department level progress toward achieving DOD IT goals. The outcome of this collaborative and iterative process will be improved IT management at all levels based on the use of performance measures.

3.9.3.2 CIO Performance Measures Executive Pilot

The CIO Performance Measures Executive Pilot will use the DOD Guide: Managing IT as an Investment and Measuring Performance to conduct a pilot study of the select, management/control, and evaluate phases of the IT Capital Planning and Investment Process. The Executive Pilot will clearly define the management roles and responsibilities, measurement levels, processes and procedures of the select, management/control, and evaluate phases. DOD's goal is to institutionalize performance and results based management by establishing performance measures as an integral part of the overall IT Capital Planning and Investment Process, within the framework of the Government Performance and Results Act (GPRA), the Clinger-Cohen Act of 1996 (Division E), and other relevant management legislation. To accomplish this, the DOD CIO has entered into a partnership with the Defense Logistics Agency and the Assistant Secretary of Defense (Health Affairs).

The results of the study will be used to influence policy, and establish common processes and procedures for managing IT as an investment and measuring performance. The ultimate outcome is to ensure that enterprise level strategic measures, functional area mission outcome measures and program/project progress measures are prescribed for all IT investments within a disciplined and structured IT Capital Planning and Investment Process, and that the performance measure indicate how well the IT investment supports the Department's mission, goals, and objectives.

3.9.4 Installation-Level Model Metrics

A set of model metrics, and standard surveys and inventories have been developed for IT infrastructure assessment at the base level. This toolkit may be used to gauge readiness and customer service. It is now available on the web at the C3I/CIO home page: www.dtic.mil/c3i/cio. Because many installation-level user IT requirements are common, DOD

will identify government and industry benchmarks for customer service. Industry benchmarks may provide generic product and service descriptions, measurement methods, and tools, as well as comparative values to include world class performance.

3.10 References

DODD 4630.5, "Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems," November 12, 1992 **[revised draft being coordinated]**

DODI 4630.8, "Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems," November 18, 1992 **[revised draft being coordinated]**

DODD 5105.19, "Defense Information Systems Agency (DISA)," June 25, 1991

DODD 8000.1, "Defense Information Management (IM) Program," October 27, 1992 **[being revised]**

DOD Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs and Major Automated Information Systems," 15 march 1996

DOD Regulation 5200.1-R, "Information Security Program," January 14,1997

CJCSI 3137.01, "The Joint Warfighting Capabilities Assessment Process," 29 Jan 1996

CJCSI 6212.01A, "Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems," 30 June 1995

Defense Planning Guidance, March 1996

National Military Strategy of the United States of America 1997

Report of the Quadrennial Defense Review, May 1997

Joint Vision 2010, not dated

Defense Reform Initiative Report, November 1997

DOD Information Technology Management Strategic Plan, 20 March 1997

Joint DII Control Systems (JDIICS) CONOPS, 19 December 1997

3.11 Related Work Groups

DII Master Plan WG

Annual DII Conference

3.12 Office of Primary Responsibility (OPR)

The OPR for the DII is:

OASD(C3I): Mr. Kevin Meyers, 703-697-7626, DSN: 227,
kevin.meyers@osd.pentagon.mil

The OPR for the DII Master Plan is:

DISA/D52: Mr. Len Tabacchi, 703-607-6233, DSN: 327,
tabacchl@ncr.disa.mil

SECTION 4

VOIDS, DISCREPANCIES, ISSUES, AND OPPORTUNITIES

One of the purposes of the DII Master Plan is to serve as a management tool to identify voids, discrepancies, issues, and opportunities in the DII. This section addresses items identified by the Components which will be the subject of DII focus group meetings in the coming months. DII related issues are encouraged to be brought to the attention of the team members listed below as soon as they are identified.

4.1 Policy

There is an absence of published DOD policy on compatibility, interoperability, integration, and security of the DII. There are draft revisions which expand the scope of DOD Directive 4630.5, "Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems," November 12, 1992 [revised draft being coordinated]); and DOD Instruction 4630.8, "Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems," November 18, 1992 [revised draft being coordinated]). Additionally, DOD Directive 8000.1, "Defense Information Management (IM) Program, is undergoing revision. Until these documents are published and have wide dissemination, there will be incomplete acceptance and understanding of the DII and the associated responsibilities, particularly with respect to interoperability.

Clarification is needed concerning the current DOD architecture policy. Specifically, the overlaps in DOD policy on the C4ISR Architecture Framework, TAFIM, JTA, and DII COE need to be rationalized with a clear set of guidance on their use and application.

A DOD DII policy working group is being led by ASD(C3I) with participation from the Joint Staff and all DOD Components. The leader of this ongoing working group is Mr. Kevin Meyers (703-697-7626).

Another DII policy issue is the releasability of software, data structures, and the data itself. Recent operations in Europe proved the need to design releasability into our systems and data "upfront," in order to avoid delay in execution.

4.2 Management

The DII is composed of various elements each of which have a management structure and responsibilities. A clear understanding of how the DII, as a whole, is managed, is essential because of the many, and intricate, interdependencies among the DII elements; for example:

- Responsibility for functional area applications, coordinating the interfaces among them; exploiting opportunities for shared infrastructure, site surveys and databases; and coordinating implementation schedules in order to ensure cost-effective implementation and the achievement of claimed benefits that depend on more than one system or capability.

- Responsibility for coordinating the implementation of migration systems with infrastructure upgrades (particularly at the base-level) upon which optimal performance of those migration systems depends.
- The philosophy and arrangements for management of shared resources need to be addressed.

4.3 Interoperability

It is implied that interoperability only can be achieved if functional area applications are JTA, COE, and SHADE-compliant. Clarification is needed about what constitutes compliance and the criteria used to determine such compliance. It is important that systems are "born Joint" if we want to ensure that we can use them to "fight Joint."

The DII must also support the exchange of information with other government agencies, commercial sector organizations, allies, and coalition partners which may not be COE or SHADE-compliant. The framework for such levels of interoperability need to be clarified to promote a comprehensive understanding of the overall initiative. In particular, security considerations need to be addressed.

DOD currently lacks a single asynchronous transfer mode (ATM) standard. Components are reluctant to start preplanned product improvements until an ATM standard is promulgated.

The DII Master Plan needs a new section highlighting the existing and planned interfaces with information infrastructures of allied partners. The section would discuss how the DII will integrate, or not integrate, with other nations, particularly during combined and multinational operations.

For clarification purposes, the role of the Standard Operating Environment (SOE) for the Defense Megacenters should be addressed and how the SOE interrelates with the DII COE/SHADE.

4.4 Technology Insertion

While planned and anticipated technology upgrades of the DII are identified, explanations of when and how such technology insertion will be done is not addressed. Examples are the transition to shared databases, or use of the Internet and object technology. A technology "roadmap" and transition plan would be valuable.

4.5 DII Control Centers

Assured information and communications can only be achieved through positive end-to-end management control of the DII. Current DII elements have been provided by C/S/As working to optimize their own part of the DII. This has led to limitations in overall DII Control Center capabilities. The most critical of these limitations is the lack of a remote monitoring and control capability of many network elements, and the inability to maintain accurate configuration management data.

Resolution of these shortcomings requires the federation of CINC, Service, and Agency DII planning, management, and operational activities to establish a control environment that can be operationally managed end-to-end.

To begin to address these key issues, DISA developed the Joint Defense Information Infrastructure Control System Concept of Operations (JDIICS CONOPS). This document complements draft DISA Circular 310-50-5, "Operational Direction and Control Exercised by the Defense Information Infrastructure (DII) Operations Control Complex (DOCC)." The latter document is being coordinated with the C/S/As.

4.6 DII Manpower and Personnel

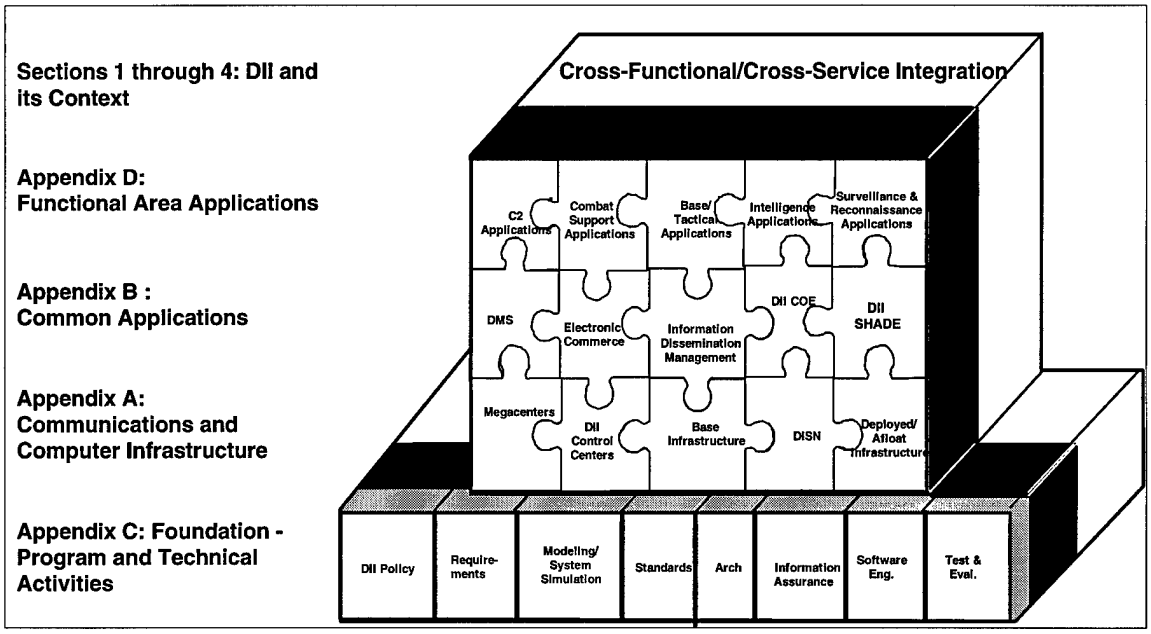
The DII Master Plan needs a new section describing the DOD workforce supporting the DII. Topics could include the current and proposed Information Technology (IT) manning levels by C/S/A, and available training for DOD IT personnel such as the Acquisition Professional Development Program, Chief Information Officer Certificate Program, AFIT Software Engineering Certificate Program, IRMC Advanced Management Program, GSA Trail Boss courses, Defense Systems Management College, etc. Links to the web addresses for each training program would significantly shorten this proposed addition to the DII Master Plan.

(This Page Intentionally Left Blank)

Appendices
to the
Defense Information Infrastructure (DII)
Master Plan
Version 7.0

Introduction to the Appendices

The appendices that follow provide an overview for each DII Element shown as puzzle pieces in the figure below. Sections in the appencies look at several aspects of each DII Element. The sections in each appendix provides a description of an element (e.g. DII COE), and address; roles and responsibilities, the baseline capabilities, the objective or long-term target capabilities, the strategy for archieving the objective capabilities, near-term initiatives, interdependencies with othe DII Elements,schedules for key milestones, requirements, and the office of primary responsibility for the section



The DII Element

The information in the appendices is intended to help integrate planning and implementaion of DII efforts across DOD. This information will allow the DII community to identify voids, discrepencies, issues, and opportunities.

APPENDIX A

COMMUNICATIONS AND COMPUTER INFRASTRUCTURE

The DII Communication and Computer Infrastructure must provide seamless connectivity for the warrior to "plug in" and obtain the information, offensive and defensive, needed to carry out any mission, at any time and at any place. The elements of the DII Communications and Computer Infrastructure are the Defense Information System Network (DISN), Enterprise Information Processing, DII Control Centers, Base and Deployed/Afloat Communications and Computer Infrastructure, and Intelligence Community Infrastructure.

DISN

DISN is the subset of the DII primarily providing information transport services both within the DII and across DII boundaries. It is transparent to its users, facilitates the management of information resources, and is responsive to national security and defense needs under all conditions in the most efficient manner. DISN provides dynamic routing of voice, text, imagery (still through full motion), and bandwidth services on a fee-for-service basis. All the other DII Elements will depend on DISN to provide the interconnecting global network to transport information. The C/S/A is responsible for operating DISN on their respective sustaining bases and deployed forces, while DISA systems will provide the long-haul connection between the bases and from the bases to the deployed forces.

DISN is being structured to satisfy evolving requirements in response to changing military strategy, changing threat conditions, and advances in information and communications technology. DOD transport of information is currently accomplished worldwide by an assortment of individual legacy communications systems. The goal architecture represents a graceful technological evolution from DOD owned and operated networks to the use of commodity services wherever possible. A commonality of architecture and standards between fixed and deployed systems will comply with the fully integrated and interoperable environment envisioned in the DII and C4IFTW. For further details see Section A.1.

Enterprise Information Processing

The DII provides the computing infrastructure for DOD. This includes enterprise computing, base level computing, and deployed computing to support all DOD missions, including command and control, direct combat support, business operations, and intelligence. The DII is composed of many disparate underlying computing configurations, designed and implemented at different times to meet different requirements. This heterogeneity will continue to exist, given the varying requirements of DOD users and the distributed execution authority within DOD. To meet the computing goal of evolvability within this heterogeneous environment, the DII is moving to a distributed, three-tiered architecture that separates data, applications, and presentation.

To ensure that interoperability, reuse, and security goals are met, the DII computing resources rely on the DII COE and the DII SOE to provide standardized access through publicly-defined interfaces to common infrastructure services such as data management (SHADE),

communications (DISN), system management (DIICC), EC/EDI, messaging (DMS), and security.

The enterprise information processing element for the DII is based on the Defense Megacenters (DMCs) and Regional Support Centers. These centers provide information processing services in support of DOD functional communities on a fee-for-service basis. The infrastructure supports communications networks, computers, operating and application software, database management, and other capabilities that offer a wide range of distributed customer services and products. These range from support of sophisticated C4I, warfighter, and scientific applications through routine business and office support systems. Services include centralized and distributed on-line and batch processing support, scheduling, secure computing, data storage and retrieval, job control and cataloged procedures, change control, management of applications software and operating systems releases, and computer products distribution. The Regional Support Centers will provide customers with local information technology services. Global communications between processing centers and bases/deployed/afloat C/JTF will be provided by DISN.

Following recommendations from the Quadrennial Defense Review mainframe information processing conducted by the Defense Megacenters is being consolidated into 5 DMC's and one legacy site. Regional Support Centers will be established at 15 sites to support local customers. For further details on Enterprise Information Processing see Section A.2.

DII Control Centers

The current system and network management activities of DISA, the Services, and other Agencies are accomplished using a variety of disparate systems at many different locations. Coordination and information sharing between management and control systems and centers are on an ad hoc basis, with near-real time reporting of status in accordance with DISA established policies.

The Objective DII Control Center Concept will provide end-to-end management of the DII technical infrastructure. Responsibility for integrated management of the DII is shared among DISA, the Services, and other Agencies. The principle parts of the Objective DII Control Centers are:

- Global Operations and Security Center (GOSC). The GOSC executes management and operational oversight of the DII. This includes ensuring that policy, standards, and guidance for systems and network security, operations and management, and the standards as developed by DISA, the Services and Agencies are applied and enforced.

- Regional Operations and Security Centers (ROSCs). The ROSCs execute the systems and network management and operational control for a specific geographic AOR. Control DISN backbone, provide theater Information Warfare (IW), Defense Message System (DMS), Global Command and Control System (GCCS) support and view certain local components of the DII.

- Local Control Centers. The LCCs (which include base-level control centers and consolidated local area control centers) execute network and system management and

operational control for a subset of the Regional responsibilities. This subset may concern a single or multiple operation, system installation or facility, or a number of installations.

Additional control centers are established for specific functions. These include; Systems Management Centers (SMCs) supporting DMCs, Defense Continuity of Operations (COOP) and Test Facility (DCTF), the Global Command and Control System Management Center (GMC), and theater control centers like the South West Asia (SWA) ROSC. For further details see Section A.3.

Base and Deployed/Afloat Communications and Computer Infrastructure

While DISA has responsibility for the DOD-wide portion of the DII communications and computing infrastructure, the extension of these functions to base, deployed and afloat users is the responsibility of the C/S/As. The Services in particular have Title 10 responsibilities to man, train and equip their forces, this includes elements of the DII communications and computing infrastructure. The challenge is to ensure the numerous single service equipment programs are interoperable, are procured to a common set of standards, and function within a DOD wide technical and operational architecture. It is also important that interdependencies between C/S/A's individual programs are clearly identified if the aim of a seamless DII is to be achieved. Details of Service programs and initiatives are now included in Section A.4.

Intelligence Community Communications and Computer Infrastructure.

The fundamental mission of the Intelligence Community (IC) is to support military and government operations by providing objective and timely intelligence to both National and Tactical consumers, to include; Executive-level decision makers; Joint Task Force and Combined Task Force Commanders; Command, Control, Communications, Computers and Intelligence (C4I) analysts; and warfighters. The IC is currently in the process of defining and developing a new information systems strategic plan, based on an operational concept of a more agile intelligence enterprise. This will satisfy intelligence requirements by managing IC resources more efficiently and adapting to change more readily. For further details see Section A.5.

Communications and Computer Infrastructure - Near Term Goals

- Release RFPs for OCONUS DISN services
- Revise DMC schedules to reflect QDR recommendations
- Establish information processing Regional Support Centers
- Consolidate DII Network Management at the ROSCs
- Obtain Service/Agency concurrence with the Joint Defense Information Infrastructure Control Concept of Operations (JDIIC CONOPS)
- Install DoDIIS COE infrastructure

(This Page Intentionally left Blank)

APPENDIX B

COMMON APPLICATIONS

Common Applications are application programs which provide capabilities that are used by all functions and organizations. They include messaging, electronic commerce, (e.g., procuring, shipping, provisioning, and making payments). Common Applications such as DMS and EC/EDI rely on the DII communication and computer infrastructure to provide information processing and information transport services. Although DMS and EC/EDI are applications programs, they are different from functional applications described in Appendix D; since **Common Applications** provide services that cross functional and organizational boundaries.

The Defense Message System (DMS) program's primary objective is to reduce cost and staffing by eliminating the resource intensive and archaic Automatic Digital Network (AUTODIN) system. A secondary objective is to improve support to the warfighter by implementing advanced messaging and directory services, building on commercial products, and incorporating international standards. Not every function provided by AUTODIN will be replicated on DMS.

The DOD functions as virtual enterprise utilizing **Electronic Commerce** to support its global mission. By developing and exploiting EC technology to conduct all phases of the business process, and using the Electronic Commerce Infrastructure (ECI), DOD can execute the National Military Strategy from peacetime, through mobilization, to sustaining warfighting capabilities, supporting the Warfighter.

The Defense Information Infrastructure Common Operating Environment (DII COE) provides a set of integrated support services for mission area application software, and a corresponding software development environment. The DII COE provides architecture principles, guidelines, and methodologies which assist in the development of mission application software by capitalizing on the infrastructure support service.

The Shared Data Environment (SHADE) supports interoperability of functional applications at the data level among the functional areas needed to provide a fused "ground truth" picture of the battlespace. Services will include a central repository of standard data elements, common procedures and tools to identify, collect and store common data elements; with built in data quality and integrity, and the secured ability to enter data only once, but share it across functions and organizations.

Information Dissemination Management. The military application of commercially developed high bandwidth transmission paths, such as Direct Broadcast Service (DBS) and Very Small Aperture Terminals (VSATs), and the convergence of individual stovepipe communications paths into the DISN has created the need for an integrated information management process. The ASD/C3I recognized this need and tasked DISA with the development of a plan for addressing Information Dissemination Management.

Relationship of the NII And The DII provides a description of the National Information Infrastructure (NII) and its relationship with the Defense Information Infrastructure (DII). The NII is defined as a seamless web of communications networks, computers, databases and

computer electronics that will put vast amounts of information at the user's fingertips. Technological advances over the past ten years in computer processing, storage, networking, transmission, and graphical user interfaces have led to the advancement of the of the concept of the NII to encompass all the communications and information processing networks that serve U.S. citizens, businesses, and government.

Future Services. The National Military Strategy calls for fused information systems that enhance our ability to dominate warfare. The DII must provide the warfighter leverage attainable from modern reconnaissance, intelligence collection and analysis, and high-speed data processing and transmission. Requisite leading edge technologies will be developed through the Defense Advanced Research Projects Agency (DARPA)/DISA Joint Program while new information services will be continually provisioned through Global Command and Control System (GCCS), Defense Information System Network (DISN), EC, and DMS programs.

Near-Term Goals

- DMS Regional Nodes installation completion NLT July 1998
- DMS Combined Communications Electronics Board (CCEB) Pilot Program scheduled for completion 1998
- EC software release of Version 2.0 to the Electronic Commerce Processing Node (ECPN)
- Release COE Version 4.0
- Implementation of SHADE Test and Integration Process Data
- Release SHADE Infrastructure Tools – Runtime Tools Version 3.0
- IDM support for Global Broadcast Service (GBS) CONOPS Theater Information Managers (TIMs)

APPENDIX C

FOUNDATION - PROGRAM AND TECHNICAL ACTIVITIES

All the Elements of the DII (**Technical Infrastructure, Value Added Services,** and **Functional Area Applications**) rely on common policy, technologies, and tools to advance through stages of consolidation, integration, and capability enhancement. **DII Technology Support** elements of the DII provide these building blocks. The foundation elements of the DII include: DII Policy, Requirements, Modeling and Simulation, Standards, Architecture, Technology Base, Software Engineering, Test and Evaluation, and Joint Spectrum Management.

- **DII Policy**. The concept of the Defense Information Infrastructure (DII) was introduced in the Defense Management Report Decision No. 918 (15 September 1992). The major themes of DII policy thus far have concerned implementing business process reengineering, moving to migration systems and standardizing data. These tasks deal with the functional processes and supporting application software which normally should drive the requirements for technical infrastructure services like communications and processing.

- **Requirements**. Fulfillment of the C4IFTW vision depends on the efficient identification and processing of the Joint Staff/CINC/Service/Agency (C/S/A) requirements needed to support the Warfighter and the subsequent distillation of those goals into cross-functional/cross-service capabilities for the Defense Information Infrastructure.

- **Modeling And Simulation.** DISA has established a capability for C4I modeling, simulation and assessment for joint service activities and DISA-initiated DII plans and programs. C4I Modeling, Simulation and Assessment (MS&A) supports concept and policy development, DII element acquisition and deployment, and DII core operations. Customers for this support include senior-level decision makers in DOD. MS&A is used to analyze scenarios for the C4I environment such as: (1) deployment of force structure requirements and options; (2) studies, analyses, network assessments and evaluation of forces, plans, programs, and strategies; (3) war games and interagency simulation in support of Joint Staff and CINCs; (4) major acquisition program evaluation, such as for DISN/GCCS/DII.

- **Standards.** DISA is the DOD Executive Agent for Information Technology (IT) standards and is responsible for making sure that the appropriate IT standards are available and used throughout all DOD communities. The CINC, Service and Agency initiatives that support the overall IT standards leadership and management include: 1) cooperation through the DOD-wide Standards Coordinating Committee (SCC); 2) the championing of DOD (i.e. DII) requirements to voluntary standards community; 3) accelerating and improving the standards process; 4) harmonizing standards among DOD communities.

- **Architecture.** The DII architecture influences DII technical decisions made by developers

across DOD. It provides a sound, cost-effective integration framework leading to efficient execution of military operations through vertical and horizontal interoperability of C/JTF and CONUS based forces. The DII architecture is developed in accordance with the TAFIM and is supported by the detailed technical specifications for the DII Common Operating Environment (COE).

- **Technology Base.** The Warfighter requires real-time information systems that are interoperable and available anywhere, anytime. This requirement can only be met by taking advantage of leading edge technologies. DISA has joined with the Defense Advanced Research Projects Agency (DARPA) to form an Advanced Information Technology Services (AITS) Joint Program Office (JPO) to expedite and smooth the transition of information technology (IT) from research and development into the "real world" and provide the Warfighter access to leading edge commercial capabilities sooner.

- **Software Engineering.** Software engineering technologies that benefit all DII Elements include: (1) process reengineering; (2) software and systems engineering tools and environments; (3) software reuse; and (4) information engineering.

- **Testing and Evaluation.** Testing and evaluation are needed to ensure the information needs of the Warfighter are met in both the current and future DOD environments. DII evaluations determine standards compliance and the extent/success of system integration. The Joint Interoperability Test Command (JITC), has the overall responsibility to coordinate the test, evaluation, analysis, and assessment activities associated with the DII.

- **Joint Spectrum Management.** The Joint Spectrum Center (JSC) serves as the DOD focal point for electromagnetic spectrum management matters and electromagnetic environment effects (E3) in support of the United Commands, Military Departments and Defense Agencies in planning, acquisition, training, and operations.

- **Information Assurance (IA)** is information operations that protect and defend information and information systems by ensuring their confidentiality, integrity, availability, authentication, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities.

NEAR-TERM GOALS

- **DOD Directive 4630.5, "Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems"** is being revised to cover all of the DOD and not just the C4I community. A draft DODD 4630.5 has been formally staffed and will supersede the existing Directive when finalized and

published. Additional changes are being incorporated to include the responsibilities of ITMRA legislation. It will promulgate policy for information interoperability and will formally define the DII.

- **DODI 4630.8,"Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems,"** has been staffed at the same time as DODD 4630.5, and similarly extends implementation to all functional areas.

- Develop the JTA Vers 2.0.

- Field the C4ISR Architecture Framework, develop lessons learned and incorporate these into Version 3.0 of the Framework. This product represents a consensus approach to the development of Information Technology (IT) architectures.

APPENDIX D

FUNCTIONAL AREA APPLICATIONS

Functional Area Applications are software developed by the Command and Control, Intelligence and Mission Support functional communities such as:

- Distribution Standard System (DSS): Logistics community;
- Mechanization of Contract Administrative Services (MOCAS): Procurement community;
- Defense Civilian Personnel Data System (DCPDS): Civilian personnel community;
- Defense Blood Standard System (DBSS): Health community;

Historically, Functional Area Applications have been developed without adequate coordination within a functional community. Thus, there are usually multiple applications operating in different Commands, Services and Agencies performing essentially the same functions. This results in duplicate applications and infrastructure (people, equipment, physical plant, etc.) with significant waste of resources across the DOD.

The lack of coordination has also resulted in the fact that these duplicative applications frequently use the same data but store them in incompatible formats. The result is data which can only be shared within the community by printing it out and reentering it into each stovepipe system. Again, a significant waste of resources.

FUNCTIONAL MIGRATION

The Integration activity in the DOD is attempting to remedy this situation. It is based upon proven private sector processes, techniques, and tools. Redundant and wasteful processes are eliminated. Processes are then realigned for optimum execution and the overall process is streamlined. COTS products are used whenever possible to satisfy Functional Requirements.

Data sharing among applications is accomplished in the long run by developing standardized data elements. In the near term, data sharing is accomplished through the use of Middleware. Middleware is COTS software that allows the user to see data presented on the same screens he used on an old stovepipe application while the data is actually stored, retrieved, and processed on a shared application know as a Migration System. This allows consolidation of duplicate systems while gradually transitioning processes and work flows to new more effective ways of doing business.

Migration systems, middleware, and the collocation of migration systems at the Megacenters will allow cross functional integration of applications in the future. The principle has been proven in prototype demonstrations already. Cross-functional integration of applications allows data from one functional community to be immediately used by applications belonging to another functional community. For instance, when an individual moves, change of address forms must be filed with many different offices (e.g. payroll, base locator, personnel, health care office) every form filed must be entered by data entry clerks into each stovepipe system. Integrating Functional Area Applications to share common data means that the change of address needs to

be made only once, possibly on the employee's own workstation. The individual's new address would be available instantaneously to all functional communities serving that person's needs.

FUNCTIONAL INTEGRATION

Frequently, decision makers do not see why it is important to integrate Functional Area Applications or how this will improve warfighting performance. One example of how inefficient, unintegrated stovepiped applications can hamper the Warfighter was experienced during Operations Desert Shield and Desert Storm. Supply officers reordered materials several times because they couldn't get timely information about where their orders were in the supply pipeline. When supplies arrived, many times support troops had to unload containers to find out their contents and destination, then reload them. This resulted in unnecessary delays, increased strain on limited U. S. lift capacity, and tying-up manpower that could have been used for other missions. The TAV effort within the Logistics community is underway to remedy this problem.

Another serious issue confronting the Commander is his/her troops' quality of life. Integration of Functional Area Applications will not only provide a fused picture of the battlespace, it will also simplify the paperwork burden and improve the timeliness of how financial, health, and human services are provided to the soldier, sailor, airman and marine. It has been estimated that the average Reservist spends 24% of duty time dealing with personal administrative paperwork. That is time that could certainly be better spent in training. Information systems can improve quality and timeliness of services that pay, house, feed, heal, educate, inform, and recreate the Warfighter both at home and when deployed. They can ease some of the strain on the best and brightest in whom we have invested tens of millions of dollars in training. They affirm our commitment to Warfighters and their families and will weigh positively in their reenlistment decisions.

NEAR-TERM GOALS

- Implement the approved GCCS plan (to Version 4.0 release).
- Install DODIIS COE infrastructure
- Migrate Procurement Functional Area to SPS/DPACS and SPS/MOCAS.
- Implement TRICARE in the Health Functional Area.
- Deploy the standard Civilian Personnel Information System.
- Complete the Modeling and Simulation Resource Repository in the Test and Evaluation Functional Area

Complete migration to the MIS for the Nuclear, Chemical, and Biological Defense Program.